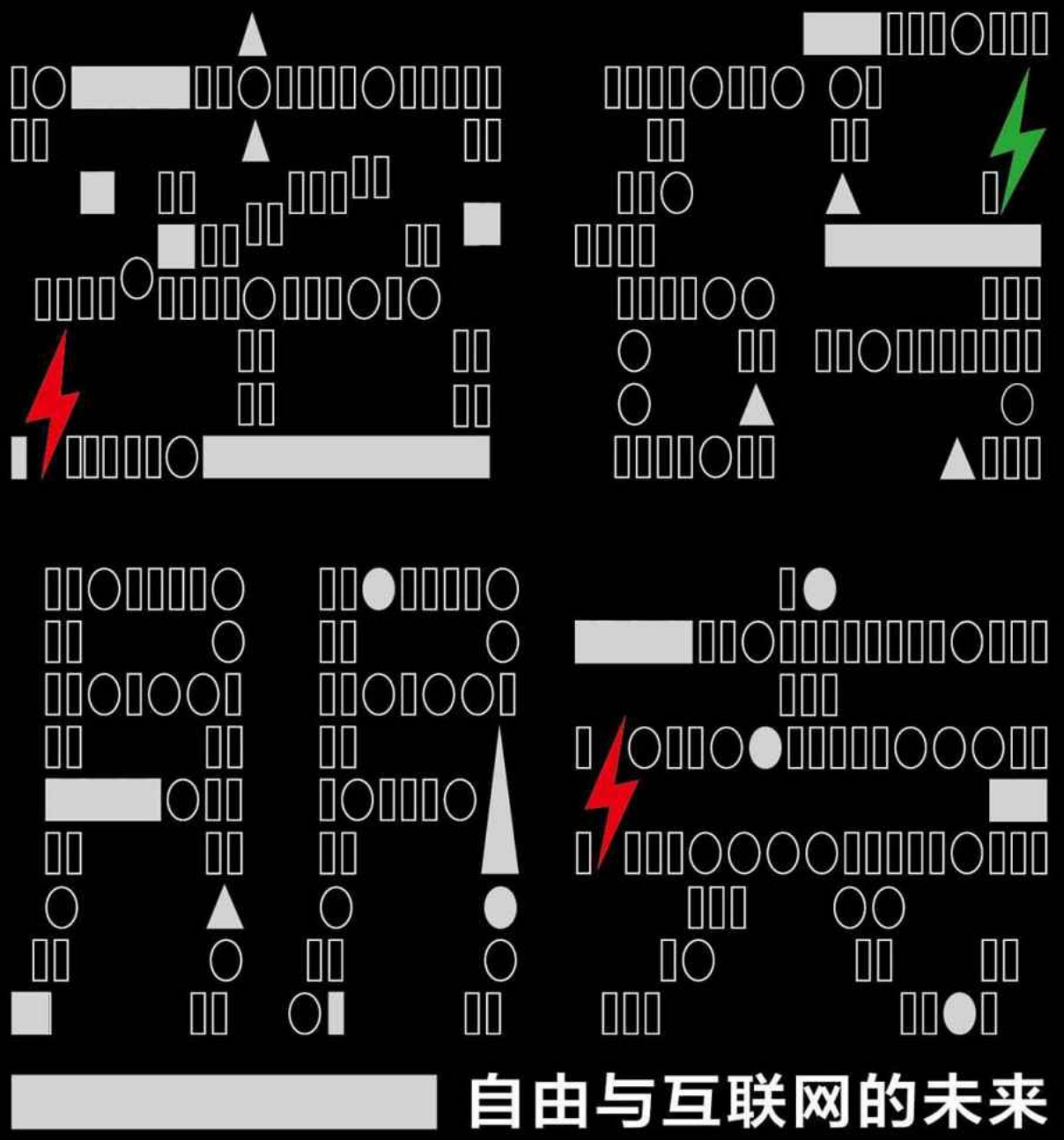


自由与互联网的未来

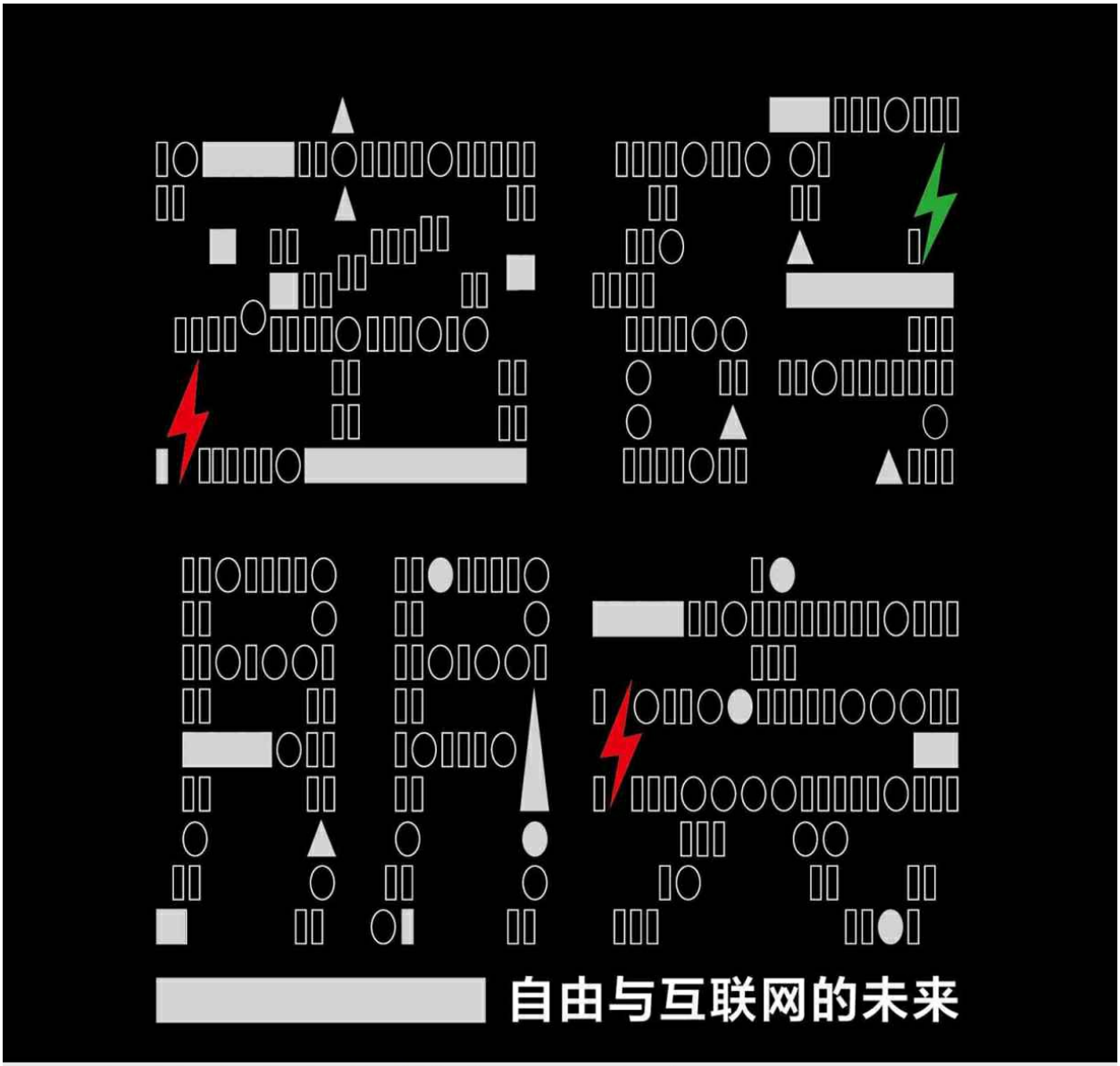
[澳] 朱利安·阿桑奇 —— 著　　Gavroche —— 译

当大规模监控对全球文明构成威胁

加密才是新世界的未来法则

奥利弗·斯通、斯拉沃热·齐泽克、约翰·皮尔格 | 联合推荐

中信出版集团



[澳] 朱利安 · 阿桑奇 —— 著　　Gavroche —— 译

当大规模监控对全球文明构成威胁

加密才是新世界的未来法则

奥利弗 · 斯通、斯拉沃热 · 齐泽克、约翰 · 皮尔格 | 联合推荐

中信出版集团

密码朋克

——自由与互联网的未来

[澳] 朱利安·阿桑奇 著
Gavroche 译

中信出版社

目录

什么是密码朋克？

密码朋克提倡通过使用密码术及其类似手段来实现社会和政治改革。[1] 该运动形成于20世纪90年代早期，在90年代的“密码战争”（cryptowars）和2011年的互联网之春时期最为活跃。“密码朋克”（cypherpunk）这个术语来自“cipher”（密码）和“punk”（朋克），在2006年被收入《牛津英语词典》。[2]

[1] 简单地说，密码学（cryptography）这个术语来自希腊语的“密写术”（secret writing），是一种通信编码措施。

[2] “Oxford English Dictionary Updates Some Entries & Adds New Words;Bada-Bing, Cypherpunk,and Wi-Fi Now in the OED”，载于ResourceShelf，2006年9月16日，http://web.resourceshelf.com/go/resourceblog/43743（访问于2012年10月24日）。

引言
对密码武器的一个呼吁

本书并非宣言，这已为时太晚。本书是一则警告。

世界已经不是在滑向，而是在奔向一个新型的跨国反乌托邦。这种发展尚未被国家安全领域之外的人正确认知。它被隐藏在秘密、复杂性和小尺度之中。互联网——我们最伟大的解放工具——已经转变成前所未见的极权主义的最危险的推进器。互联网正在威胁人类文明。

这些转变是悄然而至的，因为正在全球监控产业中展开工作的那些人没有说出真相的动机。如果任其在先前轨道上继续发展，数年之内，全球文明将会变成一个后现代的监控型反乌托邦，除了具备最好技术的那些人，其他所有人都无处可逃。事实上，我们已经置身于此了。

很多作者思考过互联网对全球文明的意义，然而他们错了。他们错了，是因为他们不具备亲身体验而获得的视角和敏感；他们错了，是因为他们从未遭遇敌人。

我们遭遇过敌人。

六年来，维基解密与几乎所有大国作战。我们学会了从一个局内人的视角来观察这种新型监控型国家，因为我们揭露了它的秘密。我们从参战者的视角来看待它，因为我们不得不保护我们的人员、我们的资金以及我们的信息源；我们从全球视角来看待它，因为我们的人员、资产和信息几乎来自所有国家；我们从一个时代的视角来看待它，因为我们已经与之斗争多年，并一次又一次地见证了它的倍增和蔓延。这是一种看不见的寄生虫，从社会中长大，越长越肥，并嵌入了互联网。它正在颠覆这个星球，正在传染每一个国家，甚至每一个人。

我们需要做什么？

过去，在现已不复存在的一个地方，我们，年轻的互联网的建设者

和公民们，讨论着新世界的未来。

我们看到，我们的新世界将改善所有人之间的关系，而由人们交流信息、经济和权力的方式定义的国家性质也将被改变。

我们看到，现存的国家结构和互联网的结合将引发国家性质的改变。

首先，要记住，国家是强制性权力在其中流动的系统。国家内的各个派别也许相互竞争以谋求支持，但这只是导致了一种民主的表象，而国家的基础是系统性地运用或规避暴力。土地所有权、财产权、租金、股息、税收、法院罚款、审查、版权以及商标，这一切，都是由国家的暴力威胁来强制执行的。

大多数时候，我们都不会注意到暴力离我们有多近，因为我们所有人都为了免遭暴力而让渡了权利。就像水手嗅到微风，我们很少思考我们眼前的世界是如何被表面之下的黑暗支撑起来的。

在互联网的新空间中，强制性权力的调节器将是什么？

提出这样一个问题真的有意义吗？在这个非现实的空间里，在这个理念和信息似乎自由流动的柏拉图国度里，也会存在强制性权力的概念吗？一种能够修改历史的权力，一种能够窃听电话的权力，一种能够分裂人民的权力，一种能够将复杂性分解并筑起高墙的权力，就像一支占领军一样的权力？

互联网的柏拉图本性，即理念和信息的流动，被它的物质起源玷污了。互联网的基础是跨越大洋海底的光缆，是在我们头上旋转的卫星，是安置在从纽约到内罗毕的城市建筑物中的计算机服务器。就像用三尺之剑杀死阿基米德的士兵，同样，一个武装的民兵也能威胁西方文明发展的巅峰、我们的柏拉图国度。

互联网的新世界，从粗暴的原子构成的旧世界脱胎而出，渴望着独立。但是，国家及其盟友行动起来，通过控制互联网的物质基础，夺取了对我们新世界的控制权。国家，就像油井周围的一支军队，或者边界上的关税代理人，向我们索取贿赂，他们将很快学会利用其对物质空间的控制，夺取对我们柏拉图国度的控制，这将阻碍我们梦寐以求的独立。进而，通过控制光纤线路、绕地卫星和地面接收站，大规模拦截我

们新世界的信息流——这个新世界的本质——即便每个人、每一种经济和政治关系都欢迎这个新世界。国家将渗入我们新社会的经脉，吞噬每一种表达和交流的关系，吞没人们阅读的每一个网页、发送的每一条信息以及搜索的每一个概念，每天拦截数十亿条信息，然后将这些权力梦寐以求的信息，永久地存储在一个巨大的机密仓库里。再然后，国家会一次又一次开采这些宝藏、这些搜集到的人类个体的智力创造，利用前所未有的复杂搜索和模式发现算法，充实这些宝藏，将拦截者与被拦截的世界之间的不平衡不断扩大。最后，国家会将他们从中所学到的运用到现实世界，去发动战争，去发动无人机攻击，去操纵贸易和联合国的委员会，去为产业界、局内人和朋党亲信的巨大关系网牟利。

但是，我们发现了一个工具，我们抵抗全面统治的一个希望，一个结合勇气、洞见和团结的希望，让我们可以利用它来进行抵抗。一项来自我们所生活的物质宇宙的奇异的属性。

宇宙相信加密。

加密容易，解密难。

我们发现，我们可以利用这项属性去创建新世界的法律。让我们的新柏拉图国度从它的卫星、海底电缆和控制器中脱身而出。让我们的空间在密码之幕背后得以加固。让我们创造一片新的国土，将那些物质现实的控制者阻拦在外；为了跟随我们，进入我们的领土，他们将耗尽无穷资源。

以这种方式，我们宣示独立。

曼哈顿计划的科学家们发现，宇宙允许原子弹的制造。这并非一个显而易见的结论。核武器也许并不属于物理定律的范畴。然而，宇宙相信原子弹和核反应堆。它们是宇宙所赐福的现象，就像盐、海洋或星辰。

与之类似，我们这个物理宇宙的一种属性，使得个人或团体能够可靠地、自动地对事物进行加密，即便是地球上最强大的超级霸权以最强烈的政治意愿动用所有的资源，也无法解密。人们之间的加密通道能够联结在一起，创造出免受外在国家强制性力量干扰的区域，免于大规模拦截，免于国家控制。

通过这种方式，人们可以用自己的意志反抗一个充分动员的超级霸权的意志，并且赢得胜利。加密的是这种物理定律的一个体现，它不听从国家的咆哮，甚至也不听从于跨国监控型反乌托邦。

世界必须如此运作，这并非显而易见。但宇宙以某种方式向加密微笑。

密码术是非暴力直接行动的终极形式。

有核国家可以对数百万人施加无限暴力，然而强大的密码术意味着一个国家——即便是能够施加无限暴力的国家——也无法打破个人保守秘密的意志。

强大的密码术能够抵抗无限施加的暴力。任何暴力都无法解决一道数学问题。

但是，我们能否利用关于世界的这个奇异事实，将它建造成互联网的柏拉图国度的基石，使人类在此得到独立和解放？随着社会与互联网的融合，这种自由能否反作用于物理现实，从而重新定义国家？

我们要记住，国家是决定强制性权力如何持久运用，以及用在何处的系统。

这种强制性权力能够在多大程度上从物理世界渗透进互联网的柏拉图国度，这个问题将由密码术和赛博朋克的理想来解答。

随着国家与互联网的融合，我们文明的未来将成为互联网的未来，我们必须重新定义权力关系。

如果我们不这么做，互联网的普世性将让全球人类逐渐消失在一个大规模监控的天罗地网中。

我们必须发出警告。本书就是守夜人在黑夜中的一声呐喊。

2012年3月20日，在等待引渡的软禁中，我在英国与三位朋友，也是志同道合的守夜人同伴会面，或许我们的齐声呐喊能够唤醒这座城镇。我们必须就我们所知交换意见，而这也给予你——读者——一个机会，去理解正在发生的事，并对此采取行动。

是时候了，拿起我们新世界的武器，为我们自己，为我们所爱之人而战。

我们的任务是在可能的地方争取自决，在不可能的地方阻止乌托邦的到来，如果这些都失败了，那就去加速它的自我毁灭。

朱利安·阿桑奇
2012年10月于伦敦

讨论参与者

朱利安·阿桑奇（Julian Assange），维基解密[1]的主编和创始人。作为密码朋克邮件列表的最初贡献者，朱利安·阿桑奇是当今世界最著名的密码朋克哲学倡导者之一。他通过维基解密所做的工作为密码朋克的传统信条“弱者要隐私，强者要透明”（Privacy for the weak, transparency for the powerful）增添了政治砝码。尽管他最耀眼的工作是对言论自由的强力实践和推动权力机构的透明和问责，但他同时也是对国家和公司侵犯个人隐私的尖锐抨击者。阿桑奇创建了众多遵循密码朋克哲学的软件项目，包括最早的TCP/IP端口扫描器strobe.c，可拒绝加密文件系统rubberhose，以及维基解密的原始代码。[2]阿桑奇少年时代就已是一名早期的计算机和网络安全研究员，那时，某些黑客行为还没有被法律认定为犯罪活动。之后的（20世纪）90年代，他成为澳大利亚的活动家和互联网服务提供商，同时还与赛利特·德累福斯（Sulette Dreyfus）合著了关于国际黑客运动历史的《地下》（*Underground*）[1]一书，电影《地下：朱利安·阿桑奇的故事》（*Underground: The Julian Assange Story*）据此改编。[3]

雅各布·阿佩尔鲍姆（Jacob Appelbaum），位于旧金山的创客空间“噪声桥”（Noisebridge）的创办者，柏林混沌计算机俱乐部（Chaos Computer Club，CCC）的成员和开发者之一。[4]雅各布还是Tor项目的推广者和研究员，这是一个旨在帮助所有人抵抗监控和规避互联网审查的匿名上网系统。[5]过去十年，他的主要活动是推动环境保护和人权运动。为了这个目标，他已经在从计算机取证到医用大麻的多个领域发表了有关新型安全、隐私和匿名的研究。

雅各布相信毫无例外每个人都有自由阅读和自由发言的权利。2010年，当朱利安·阿桑奇无法到纽约发表一个讲话时，雅各布代其发言。从此以后，他以及他的朋友和家人便遭到美国政府的骚扰：在机场遭受执法官员的盘问、侵犯性搜身，并被暗中威胁即将遭受监狱强奸，他的设备被没收，他的在线服务项目受到秘密传讯。这些措施没能让雅各布屈服，他继续进行法律斗争，同时仍是言论自由的公开倡导者和维基解密的积极支持者。

安迪·米勒–马贡（Andy Müller-Maguhn），是位于德国的混沌计算机俱乐部的长期成员、前董事会成员兼发言人。[6]他是欧洲数字权利组织（EDRI）的联合创始人之一，这是一家旨在加强数字时代人权的非营利性组织。[7]2000年到2003年，他被欧洲互联网用户推选为互联网名称与数字地址分配机构（ICANN）的欧洲地区总监，该机构负责为全世界互联网的“名字和数字”运行制定政策。[8]他还是一位电信和其他类型监控方面的专家，通过他的维基项目buggedplanet.info[9]对监控产业进行专业调查。安迪在密码通信领域展开工作，并与其他人共同创办了加密电话（Cryptophone）公司，该公司向商业客户销售安全语音通信设备，并在网络架构环境中提供战略咨询服务。[10]

热雷米·齐默尔曼（Jérémie Zimmermann），公民诉求团体La Quadrature du Net的联合创始人和发言人，该组织是欧洲地区捍卫在线匿名权的最著名的组织，同时也致力于促进人民对互联网自由的管制和攻击的认识。[11]热雷米致力于为公众参与公共辩论以及推动改革开发工具。他投身于版权战争（copyright wars），这场论战围绕网络中立性和其他对自由互联网的未来有关键影响的监管议题展开。最近，他的组织La Quadrature du Net在欧洲政治中取得了一项历史性胜利，他们召集的公众运动在欧洲议会上成功击败了《反假冒贸易协定》（ACTA）。参与作为本书基础材料的讨论后不久，热雷米在离开美国时遭到两名FBI（美国联邦调查局）官员的阻拦，并被盘问与维基解密有关的问题。

注释

1. 维基解密：http://wikileaks.org。

2. 更多关于rubberhose文件的信息，参见赛利特·德雷福斯：“The Idiot Savants’ Guide to Rubberhose”，http://marutukku.org/current/src/doc/maruguide/t1.html（访问于2012年10月14日）。

3. 更多关于图书《地下》的信息，参见：http://www.under-ground-book.net；更多关于电影《地下：朱利安·阿桑奇的故事》的信息，参见：Internet Movie Database：http://www.imdb.com/title/tt2357453/（访问于2012年10月21日）。

4 . “噪声桥”是一个位于旧金山的黑客空间，为技术创意产品提供基础设施，由其成员联合运营：https://www.noisebridge.net/wiki/Noisebridge；柏林混沌计算机俱乐部是混沌计算机俱乐部的柏林分支机构，参见：https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin。

5 . Tor项目：https://www.torproject.org。

6 . 混沌计算机俱乐部是欧洲最大的黑客协会，其活动包括技术研究和开发、政治竞选运动、集会活动、出版活动以及政策建议：http://www.ccc.de。

7 . 欧洲数字权利组织：http://www.edri.org。

8 . 互联网名称与数字地址分配机构（ICANN）：http://www.icann.org。

9 . 窃听行星（buggedplanet）：http://buggedplanet.info。

10 . 加密电话：http://www.cryptophone.de。

11 . La Quadrature du Net：http://www.laquadrature.net。

[1] 中译本名为《维基大战前传I：阿桑奇和他的黑客战友》（世界图书出版公司，2011年出版）。

编者按

为了加深一般读者对密码朋克的了解，我们允许每一位原始讨论的参与者对各自观点进行实质性的扩展、澄清和注释。编辑后的手稿遵循原始讨论的时间顺序。

对维基解密及相关人员的各种迫害企图的注释

以下的几点讨论，参考了近年来在维基解密及其发布活动中发生的事件。对不熟悉维基解密故事的读者来说，这些事件可能很难懂，所以需要在一开始做一番概述。

维基解密的使命是从告发者那里接收信息，向公众发布信息，同时抵抗不可避免的法律以及政治攻击。强大的国家和组织企图镇压维基解密的信息发布，这是他们的例行公事，而作为最终发布者，这也是维基解密需要面对的困难之一。

2010年，维基解密卷入了迄今为止最著名的一场信息发布事件，揭露了美军及美国政府内部对官方机密的系统性滥用。所发布的这些信息就是著名的附带谋杀（Collateral Murder）、战争日志（the War Logs）和电报门（Cablegate）。[1] 美国政府及其盟友对此的回应是一场持久的、旨在摧毁维基解密的协同行动。

对维基解密的大陪审团调查

作为维基解密发布的直接后果，美国政府发动了一场多机构参与的对朱利安·阿桑奇以及维基解密的员工、支持者和所谓的合作者的刑事调查。弗吉尼亚的亚历山德里亚（Alexandria）在美国司法部和FBI的支持下召开了一场大陪审团调查，以调查能以何种罪名对朱利安·阿桑奇及其他人提出指控，包括根据《1917年间谍法》提出阴谋罪指控。美国官员说这场调查具有“史无前例的规模和性质”。在大陪审团调查过程中，没有法官和辩护律师出席。国会委员会的听证会听取了美国国会议员的建议，认为间谍罪可以作为一种攻击“公然发布泄密信息”的记者的工具，这显示此种方式已经成为美国司法系统的一种常规手段。[2]

到本书出版之时，对维基解密的调查仍在继续。[3] 一些人已经被合法强制要求提供证据。对被控向维基解密传送信息的士兵布拉德利·曼宁（Bradley Manning）[1] 的法庭审理，揭露了FBI对维基解密的一份长达42100页的调查文件，其中大约8000页内容涉及曼宁。布拉德利·曼宁在未经审判的情况下，被扣押了超过880天。联合国酷刑问题特别调查员胡安·门德斯（Juan Mendez）正式裁定布拉德利·曼宁所遭受的是一种残酷甚至不人道的待遇，并可能近乎于酷刑。[4]

呼吁暗杀朱利安·阿桑奇并公开宣布成立维基解密专案组

大陪审团调查并不是攻击维基解密的唯一手段。2010年12月，随着电报门事件的发生，多名活跃的美国政客呼吁对朱利安·阿桑奇实行法外暗杀，包括无人机攻击。美国议员给维基解密贴上“恐怖组织”的标签，并指称阿桑奇是一名“高科技恐怖分子”和参与“赛博战争”的“敌方战士”。[5]

在伊拉克战争日志发布和电报门事件发生前夕，美国国防部成立了一个由120人组成的维基解密专案组（WikiLeaks Task Force，WTF），宣称要对维基解密“采取行动”。FBI也公开宣布成立了类似的专案组，美国中央情报局（CIA）和国务院也加入了行动。[6]

直接审查

在一项对新闻出版的史无前例的审查行动中，美国政府向互联网服务提供商施压，要求其停止对WikiLeaks.org提供服务。2010年12月1日，亚马逊从其存储服务器中删除了维基解密网站的数据，12月2日，指向Wikileaks.org域名的DNS服务中断。在此期间，数以千计的维基解密支持者复制了网站，托管了他们自己的版本，并通过社交网络分发IP地址，这种“大规模镜像”（mass-mirroring）的努力使维基解密一直保持在线。[7]

奥巴马政府警告联邦雇员，维基解密所披露的资料仍处于机密级别，即使某些世界领先的新闻机构，包括《纽约时报》和《卫报》，已经发布了这些资料。奥巴马政府通告联邦雇员，无论是通过WikiLeaks.org，还是通过《纽约时报》获取这些资料，都将被当作安全违规。[8]国会图书馆、商务部和美军等机构在他们的网络中封锁了对维基解密资料的访问。这种封锁并不仅限于公共部门。美国政府的雇员警告学术机构，想要在公共机构谋职的学生也应在其研究和在线活动中回避维基解密所披露的资料。

金融审查：银行封锁

维基解密的资金来自支持者的捐款。2010年12月，包括维萨（VISA）、万事达（MasterCard）、贝宝（PayPal）和美洲银行在内的主要银行和金融机构，屈服于美国非官方的压力，开始拒绝向维基解密提供金融服务。它们封锁了银行转账和使用主要信用卡的所有捐款，尽管这些金融机构位于美国，但它们在世界金融业中的重要地位，使得无论是美国还是世界其他国家的志愿捐助者都无法向维基解密汇款，以支持其发布活动。

正如人们所知，“银行封锁”是在一切司法和行政程序之外进行的，并且时至今日仍然存在。维基解密已在全球不同的司法管辖区内寻求主要的司法判例以求打破封锁，并取得了某些初步成果，而法律程序仍在进行当中。与此同时，维基解密在没有收入、成本上升的情况下，利用储备资金运营了近两年。

银行封锁是以权力来控制第三方之间金融交易的明确表现。这直接破坏了个人的经济自由。不仅如此，对维基解密施加的外部威胁体现出一种新的、令人不安的全球经济审查形式。[9]

某些据称与维基解密合作的人士，包括维基解密的支持者和维基解密员工的账户都遭遇了莫名其妙的麻烦，从一些小问题到整个银行账户被关闭。

对雅各布·阿佩尔鲍姆和热雷米·齐默尔曼的骚扰

2010年7月17日，朱利安·阿桑奇被安排在纽约的地球黑客大会（Hackers On Planet Earth，HOPE）上发言。他取消了计划，而由雅各布·阿佩尔鲍姆代其出席。自这次出席之后，阿佩尔鲍姆及其身边的人就遭到执法机构的持续骚扰。无论是在美国国内还是国外旅行，阿佩尔鲍姆在过境时都会经常性地遭遇拘留、搜身和盘问，而且不允许与律师联系。他的设备被没收，权利遭到侵犯，在此期间他还受到将进一步侵犯其权利的威胁。美国的多个机构都参与了对他的拘留和骚扰，从美国国土安全局、移民和海关执法局到美国陆军。在拘留时采取的施压手段甚至包括不让他上厕所。尽管如此，阿佩尔鲍姆从未被正式起诉，政府也从未告知他被骚扰的原因。[10]

2011年6月中旬，热雷米·齐默尔曼在华盛顿杜勒斯机场准备登机时，被两名自称来自FBI的官员拦下。FBI的官员向他询问维基解密的情况，并威胁要逮捕和监禁他。

在朱利安·阿桑奇的朋友、支持者或所谓合作者中，除了阿佩尔鲍姆和齐默尔曼，还有很多人遭到了美国当局的骚扰和监控，这份名单中还包括以履行其专业职责而参与到此事中的律师和记者. 。

对电子记录未经授权的没收和“Twitter传票案”

2010年12月14日，Twitter（推特）收到了一张来自美国司法部的“行政传票”（administrative subpoena），命令其交出一份可能与维基解密的调查有关的信息。这种传讯的根据是美国《通信存储法案》（The Stored Communications Act）中所谓的“2703（d）命令”［2703（d）order］。在该法律之下，美国政府声称有权强迫公开私人电子通信记录，而无须法院发布搜查令，这就有效地绕开了美国宪法第四修正案中对抵抗任意搜查和逮捕的保护。

该传票要求取得用户的名字、通信记录、地址、电话号码、银行账户明细、账户的信用卡号，还有维基解密所谓的合作者，包括雅各布·阿佩尔鲍姆、冰岛议员贝尔吉塔·扬斯多蒂（Birgitta Jonsdottir）、荷兰商人及互联网先驱霍普·洪赫莱普（Rop Gonggrijp），以及维基解密自己的信息。该传票的条款还要求Twitter不得向这些人通知该命令的存在。然而，Twitter对禁言令的上诉取得胜利，赢得了向这些目标人物通知他们的记录正被索要的权利。

2011年1月26日，Twitter向阿佩尔鲍姆、扬斯多蒂和洪赫莱普通知了传讯有关事宜，以诉讼公司凯克和范·奈斯特（Keker and Van Nest）为代表，美国公民自由联盟（American Civil Liberties Union）和电子前哨基金（Electronic Frontier Foundation）让他们的律师联合正式提出一项动议，要求撤销该命令。这就是众所周知的“Twitter传票案”[11]。阿佩尔鲍姆的律师提出更进一步的动议，要求公开美国政府企图从Twitter和其他任何公司搜集个人信息的行为的法庭记录，这些记录尚在保密之中。2011年3月11日，两项动议都被美国治安法官驳回。原告提出上诉。

2011年10月9日，《华尔街日报》披露，加州电子邮件提供商Sonic.net也收到了索要雅各布·阿佩尔鲍姆的信息的传票。Sonic对政府命令的抵抗虽然失败了，但获得许可，可以公开他们被迫交出阿佩尔鲍姆的信息这件事。《华尔街日报》同时报道，Google（谷歌）也服从了类似的传讯，但没有说Google是否就此向法院提出质疑。[12]

2011年11月10日，联邦法官驳回阿佩尔鲍姆、扬斯多蒂和洪赫莱普的要求，判决Twitter必须向司法部提交他们的信息。[13]2012年1月20日，原告再次提出上诉，对拒绝公开可能已向Twitter之外的公司所发布的命令提出质疑。[14]到本书出版之时，此案仍在进行当中。

注释

1. 附带谋杀（Collateral Murder）：http://www.collateralmurder.com；伊拉克战争日志（The Iraq War Logs）：http://wikileaks.org/irq；阿富汗战争日志（The Afghan War Diary）：http://wikileaks.org/afg；电报门（Cablegate）：http://wikileaks.org/cablegate.html。

2. “Congressional committee holds hearing on national security leak prevention and punishment”，参见美国新闻自由记者委员会报告（Reporters Committee for Freedom of the Press），2012年7月11日，http://www.rcfp.org/browse-media-law-resources/news/congressional-committee-holds-hearing-national-security-leak-prevent（访问于2012年10月21日）。

3. 更多关于维基解密大陪审团调查的信息参见独立记者阿列克萨·奥布莱恩（Alexa O’Brien）的时间轴：http://www.alexaobrien.com/timeline_us_versus_manning_assange_wikileaks（访问于2012年10月22日）。

4. “Bradley Mannin’s treatment was cruel and inhuman,UN torture chief rules”，载于《卫报》，2012年3月12日，http://www.guardian.co.uk/world/2012/mar/12/bradley-manning-cruel-inhuman-treatment-un（访问于2012年10月24日）。

5. “WikiLeaks:guilty parties ‘should face death penalty’”，载于《电讯报》，2010年12月1日，http://www.telegraph.co.uk/news/worldnews/wikileaks/8172916/WikiLeaks-guilty-parties-should-face-death-penalty.html（访问于2012年10月22日）。

6. “CIA launches task force to assess impact of U.S. cables’exposure by WikiLeaks”，载于《华盛顿邮报》，2010年12月21日，http://www.washingtonpost.com/wp-dyn/content/article/2010/12/21/AR2010122104599.html?hpid=topnews&sid=ST2010122105304（访问于2012年10月22日）。

7．“WikiLeaks fights to stay online after US company withdraws domain name”，载于《卫报》，2010年12月3日，http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns（访问于2012年10月23日）。

8．“Don’t Look,Don’t Read:Government Warns Its Workers Away From WikiLeaks Documents”，载于《纽约时报》，2010年12月4日，http://www.nytimes.com/2010/12/05/world/05restrict.html?hp&_r=2&（访问于2012年10月23日）。

9．“Banking Blockade”，载于维基解密，http://www.wikileaks.org/Banking-Blockade.html（访问于2012年10月22日）。

10．建议阅读雅各布对于自己拘留经历的书面说明，参见“Sir Space- a trip through an airport detention center”，载于boingboing，2011年10月31日，http://boingboing.net/2011/10/31/air-space-a-trip-through-an-ai.html；同样重要的还有雅各布在Democary Now上就其扣留所接受的采访“National Security Agency Whistleblower William Binney on Growing State Surveillance”，载于Democracy Now，2012年4月20日，http://www.democracynow.org/2012/4/20/exclusive_national_security_agency_whistleblower_william（访问于2012年10月23日）。

11．本案的官方名称为“有关Twitter账户的2703（d）命令：维基解密、霍普·洪赫莱普、贝尔吉塔·扬斯多蒂”［In the Matter of the 2703(d) Order Relating to Twitter Accounts: Wikileaks; Rop Gonggrijp; and Birgitta J.］。

12．“Secret orders target email”，载于《华尔街日报》，2011年10月9日，http://online.wsj.com/article/SB10001424052970203476804576613284007312问于2012年10月22日）。

13．“Twitter Ordered to Yield Data in WikiLeaks Case”，载于《纽约时报》，2011年11月10日，https://www.nytimes.com/2011/11/11/technology/twitter-ordered-to-yield-data-in-wikileaks-case.html?_r=1（访问于2012年10月22日）。

14 . “ACLU&EFF to Appeal Secrecy Ruling in Twitter/WikiLeaks Case”电子前哨基金发布于2012年1月20日，https://www.eff.org/press/releases/aclu-eff-appeal-secrecy-ruling-twitter-wikileaks-case（访问于2012年10月22日）。

[1] 现为切尔西·曼宁（Chelsea Manning）。——译者注

增加的通信对增加的监控

朱利安·阿桑奇：如果我们回顾20世纪90年代早期，作为对国家禁止密码术的回应，兴起了密码朋克运动。很多人看到，与主流媒体相比，互联网提供了一种自由的、不受审查的通信力量。但密码朋克却知道与此相对的另一种力量的出现，那就是监控一切通信的权力。现在我们看到的是增加的通信对增加的监控。增加的通信意味着，对于试图控制观念和炮制共识的人，你拥有了额外的自由；而增加的监控则限制了你的自由。

过去，只有美国、英国、俄罗斯、瑞典、法国等国政府实施监控，相比之下，现在的监控是越来越明目张胆了。现在，由于大规模监控的商业化，所有人都在搞监控，几乎所有国家都在实施监控。现在的监控正在全面普及，因为人们把他们所有的政治观点，家庭关系，以及朋友圈都放在网上。所以，不仅是通信存量的监控在增长，而且还有对更多通信的监控。此外，不仅通信量在增长，通信的类型也越来越多。各种新的通信类型，过去可能都是私人性质的，现在都被大规模拦截了。

在信息掌权者与数量越来越多的公众之间存在着一场斗争。前者是那些搜集信息的局内人，那些信息的影子政府，他们正在发展壮大，互换情报，发展彼此的联系以及与私人部门的联系；后者则把互联网当作一个可以让全人类为自己发声的公共工具。

我想思考一下我们是如何表达自己观点的。作为一个曾经涉足国家监控并理解跨国安全行业在过去二十年的发展的人，我的一大问题是，我自己对此太熟悉了，所以我不太理解如何从一个普通人的视角来看待这些事情。然而，现在我们的世界是所有人的世界，因为每个人都将他们生活的内核放到了互联网上。我们不得不以某种方式就彼此所知进行交流，在我们还能够这么做的时候。

安迪·米勒–马贡：我建议我们不必从一个公民的视角，而是以当权者的视角来看待这个问题。前几天我在华盛顿出席了一个陌生的会议，我遇到了一些佩戴德国使馆徽章的家伙。我走近他们，问道：“哦，你们是来自德国大使馆的？”然后他们说：“啊，不完全是使馆的，我们是

从慕尼黑附近来的。”后来证明，他们来自外国情报局。我在晚餐会上问他们：“那么，秘密的关键是什么？”他们告诉我：“好吧，就是延缓事件进程以便更好地控制他们呗。”这就是这类情报工作的核心，通过剥夺人们理解事件的能力来延缓事件的发展。一旦宣布某些事件是机密，就意味着你限制了通过了解事件继而有能力影响事件进展的人数。

当你从这种当权者的视角来看待互联网，过去二十年的发展就是令人十分恐惧的。他们把互联网看作一种疾病，这种疾病损害了他们的能力，他们过去用这种能力去定义现实，去定义正在发生的事，去限制人们对所发生的事情的了解，以及人们对事情的反应能力。如果你看一看，以沙特阿拉伯为例，由于某些历史偶然因素，那里的宗教领袖也正好是掌握大部分国家权力的人，他们对于改变现状的兴趣趋近于零——也许是零到负五吧。他们把互联网看作一种疾病，然后问他们的顾问们：“对此你们有何良方？如果这会损害我们的国家，我们必须对此免疫。”答案就是大规模监控：“我们需要全面控制它，我们需要过滤，我们需要知道他们所做的所有事。”于是，这就是最近二十年来发生的事情。当权者对监控进行大规模投资，因为他们害怕互联网会影响他们的统治方式。

朱利安·阿桑奇：然而，尽管有这种大规模监控，大规模的通信还是让数以百万计的人们能够迅速达成共识。如果从常态中能非常迅速地形成一种新的大规模舆论，尽管国家也许能够预计它的发展，但也没有足够的时间对此作出有效反应了。

现在，人们说，是Facebook（脸谱网）组织了2008年发生在开罗的抗议。这震惊了穆巴拉克政府，结果那些发动抗议的人也通过Facebook被追踪到了。[1] 2011年，埃及革命中所使用的最重要的文件之一，其第一页和最后一页都这样写道：“不要使用Twitter或Facebook来散发本手册。”[2] 尽管如此，还是有大量埃及人在使用Twitter和Facebook。但他们得以幸存的原因在于革命成功了。如果没能成功，那么这些人将可能处在一种非常、非常艰难的境地。而且，我们不要忘记，在革命早期，总统穆巴拉克曾经切断了埃及的互联网。事实上，互联网管制是促进还是损害了这场革命也是有争议的。有人认为它推动了革命，因为人们不得不走上大街去探听事态进展的最新消息，而一旦你走上大街，你就站出头了。而且人们受到了直接的影响，因为他们的手机和互联网都不能用了。

所以，如果革命要走向成功，就需要一群愤怒的大众，需要速度，而且需要取胜，因为一旦不能取胜，同样的基础设施既能让一种舆论共识快速发展起来，也能被用来追踪并排斥那些卷入这场舆论散播中的人。

所以，这就是在埃及发生的事，没错，埃及曾经是美国的一个盟友，但它不是英语国家情报联盟的成员，这个情报联盟包括美国、英国、澳大利亚、新西兰和加拿大。现在让我们假设一下埃及革命发生在美国——那么Facebook和Twitter上会发生什么呢？它们可能会被国家接管。一旦革命无法成功，它们就会被中央情报局和联邦调查局彻底搜查，找出那些关键的参与者。

热雷米·齐默尔曼：很难将监控与控制分开。我们需要同时应对两种对互联网的控制——政府的控制和企业的控制。

雅各布·阿佩尔鲍姆：我认为，很明显，审查也是一般意义上监控的一个副产品，无论是自我审查还是实际上的技术审查，而且，我认为将这种认识以一种非技术性的方式传播给普通人是非常重要的。例如，如果我们修一条路，就像我们建造互联网那样，每一条道路都有监控摄像头和麦克风，除了警察或成功地伪装成警察的人，没有人能接触这些设备。

朱利安·阿桑奇：他们正在这里搞这些东西，雅克，就在英国。

雅各布·阿佩尔鲍姆：你修一条路，不会在每一寸道路旁都设置只有秘密警察集团才能查看的完美监控。可以用这种方式向普通人解释：这就好比我们在互联网上修建道路，然后要求人们使用这些道路，这样当人们意识到道路的最初修建者并不总是管理道路的人，他们就能想通其中的道理了。

安迪·米勒–马贡：但这些人甚至都不修路。他们在那里盖一座花园，要求人们赤身裸体。所以现在我们在谈论Facebook了！这就是一个商业案例，让人们舒适地暴露自己的数据。

雅各布·阿佩尔鲍姆：对。人们为斯塔西（Stasi）——原民主德国的国家安全机构——效力还能拿到报酬，而他们现在靠在Facebook上的活跃度来获得报酬。区别在于，在Facebook上，人们拿到的报酬是社会资本——比如和邻居勾搭的机会——而非金钱。而且，重要的是从人的

层面来看这件事，因为它不是关于技术的，而是通过监控来实现控制。从某种意义上说，这就是一座完美的环形监狱[3]。

朱利安·阿桑奇：我对技术哲学相当感兴趣。技术不仅意味着一种科技，它也是系统性的相互作用，就像一个董事会中的多数同意，或一个议会的结构。例如，在我看来，封建制度似乎产生于磨坊技术。一旦你拥有集中的磨坊——这需要大量投资，而且在物理上很容易控制，那么最终走向封建关系就是自然而然的了。随着时间的推移，我们又发展出了越来越多的精密技术。其中一部分可以民主化，这些技术可以分享给每个人：但是大部分技术——由于其复杂性——最终都会形成盘根错节的组织集团，就像英特尔公司。也许技术的基本趋势就是要经历这些阶段，从技术的发明，到技术的集权化，再到技术的民主化——如果其原理能冲击到下一代的受教育人口。但是，我认为技术的一般趋势是将控制权集中在控制了技术的物质资源的人们手中. 。

我认为半导体制造商是一个极端的例子，它要求这种生产流程：需要完全纯净的空间，需要一座制造工厂，有数以千计的人在其中工作，他们必须穿戴防护服以防止脱落的皮肤碎屑破坏纯净的操作间，一根头发丝都不能接触半导体的生产流程。这种包括众多步骤的流程极其复杂，而且半导体制造厂商还要投入数百万小时的研究来获取这些知识。如果半导体制造厂内采用的复杂流程设计普及开来——事实上已经如此——则将成为互联网自由的基础。实际控制着半导体制造厂商的人就有能力在其中收取高额费用。

因此，支撑这场高科技通信革命——以及我们从中获得的自由——的是整个新自由主义的、跨国的、全球化的现代市场经济。从技术成就的角度来看，互联网是现代全球新自由主义经济制造出的一个制高点。支撑互联网的是光纤电缆制造商、半导体制造商、挖掘出生产这些产品所需原材料的矿业公司，以及所有保证交易发生的金融促进机构、执行私有产权法的法庭等组织之间复杂的交易互动。所以，互联网确实是处于整个新自由主义经济体系金字塔的顶端。

安迪·米勒–马贡：关于技术，在约翰内斯·古登堡（Johannes Gutenberg）[4]发明印刷术时，德国某些地区其实偶尔会禁止这项技术，而它还是在全国传播开来，因为当印刷术在一地遭到禁止，他们就会转移到另外的司法管辖区。我对此没有做过详细研究，但据我所知，他们扰乱了天主教会，因为他们是在打破教会对书籍的垄断权；而一旦卷入

法律纠纷，他们就转移阵地，去那些没有禁止这项技术的地方。在某种程度上，禁令甚至推动了这项技术的传播。

我认为，互联网的情况稍有不同，因为一方面你拥有的这些机器也可以用来作为一台生产设备，即便是Commodore　64这样的古董，在某种程度上，很多人也可以拿它去用于其他目的。

朱利安·阿桑奇：所以，你拥有的每一台小机器，都能拿来运行你自己的软件。

安迪·米勒–马贡：是这样。你也可以用它来散布观点。但是，另一方面，从哲学角度看，正如美国的电子前哨基金会创始人之一约翰·吉尔莫（John　Gilmore）在20世纪90年代初所言，当时互联网实现了全球覆盖，“网络将审查视作故障，并绕道而过”。[5]现在我们知道，那是一种结合了乐观主义观点的技术阐释，也代表了一种一厢情愿的想法和一种自我实现的预言。

朱利安·阿桑奇：但对新闻组（Usenet）来说确实如此，你可以把新闻组看成一种大约三十年前出现的多对多电子邮件系统。我简单地解释一下新闻组：你可以想象在用户和服务器之间不存在差别，每个人都能运行他们自己的新闻组服务器。你写下某个东西，把它发送给一两个人，新闻组服务器会自动查看是否已经被接收。如果还没收到，它们就会获取一份，然后把它转发给它们所连接的每一个人，如此等等。结果是这则消息涌向了每个人，每个人实际上都得到了一份拷贝。一旦任何个人遭受审查，他们只会被忽略，这不会造成多大影响。这则消息依然在所有未遭审查的人们之间传播。吉尔莫说的正是这种新闻组，他不是在说互联网，他也没有谈到网页。

安迪·米勒–马贡：当然，严格来说是这样，但对他这种说法的解读，以及这些解读的长期影响造就了一批人，他们把自己视为互联网。人们说：“这里有审查，那好，我们会绕开它。”而那些没有技术知识的政客会想：“糟糕，又来了一项新技术在限制我们对信息领域的控制。”所以，我认为吉尔莫作为密码朋克的先知之一，将事情引导到这个方向是伟大的贡献，他鼓舞了所有秘密无政府主义者的行为方式，那就是你要拥有自己的匿名通信方式，而不必害怕会被跟踪。

热雷米·齐默尔曼：在我们对技术传播的描述中，我发现了一点差异，因为在磨坊和印刷术的案例中，你不得不理解这项技术的工作原

理，而现在我们是在技术内部制造更多的控制。这种控制是内嵌的。对于一部现代计算机，在大多数情况下人们甚至不能打开它，不能了解所有的部件。而且所有的部件都被封装在一个小盒子里，你不可能知道它们都是做什么的。

安迪·米勒–马贡：因为技术复杂？

热雷米·齐默尔曼：因为复杂，也因为技术本身就不是为了让人理解的。这就是专利技术的情况。[6] 科里·多克托罗（Cory Doctorow）在他的报告《对通用计算的战争》（The Coming War on General-Purpose Computing）中对此做过描述。[7] 如果计算机是一台通用机器，你就可以对它做任何事情。你可以把任何信息处理成一个输入，将它改造成任何输出。我们现在制造了越来越多这样的机器，它们是通用计算机，却被限制而只能被用作GPS或电话或MP3播放器。我们现在制造了越来越多这样带有内嵌控制的机器，来限制用户只能做某些特定的事。

朱利安·阿桑奇：这种内嵌的控制阻碍人们去理解它，防止人们违背制造商的意图去改造它，但目前的情况甚至更糟，因为这种内嵌控制的机器还是联网的。

热雷米·齐默尔曼：对，所以它包含了监视用户和用户数据的功能。这就是为什么自由软件对一个自由社会是如此重要。

安迪·米勒–马贡：我完全同意我们需要通用机器，但今早我从柏林飞到这里时，飞机起飞中断了——我还是第一次遇到这种事。飞机驶向跑道边，然后机长说：“女士们、先生们，我们的电子系统发生了故障，所以我们决定停止起飞，然后重启系统。”我当时就在想：“该死，听起来像是Windows重启，Ctrl+Alt+Delete也许管用！”所以，实际上，我并不讨厌飞机上的专用机器，它们就做自己的事，而且做得很好。如果我坐在一架飞行器中，我可不愿意飞行员分心去玩俄罗斯方块，遭遇震网攻击[8]或其他什么的。

热雷米·齐默尔曼：飞机本身并不处理你的个人数据，它不会控制你的生活。

安迪·米勒–马贡：好吧，不过一架飞行器确实能在一段时间内控制我的生命。

雅各布·阿佩尔鲍姆：科里的论点，我觉得也可以用被这种说法很好地描述，那就是，现在不再有汽车，不再有飞机，也不再有助听器了，现在有的是带四个轮子的计算机、带机翼的计算机和帮助你听声音的计算机。这里的部分问题不在于它们是否用计算机，我们是否能检验它们的功能符合其所声称的用途，以及我们是否能很好地理解它们是如何工作的。人们经常争辩说，他们有权给这些东西上锁，并且保守秘密，他们要么把计算机造得很复杂，要么从法律上将其弄得难以理解。这其实是在对社会构成威胁，因为我们知道，人并不总是按照所有人的最大利益行事，我们也知道，人常常犯错——并非出于恶意——而把这些东西都锁起来在很多层面上都是非常危险的，并不仅仅因为人非完人。这就是事实。自由软件之所以重要，一部分原因在于，这是我们获取作为我们生活基础的系统蓝图的能力，这也是自由硬件之所以重要的原因。自由软件改善我们自由地进行可持续投资的能力，改善我们使用的系统，还决定着这些系统是否能如预期的那样工作。

但即便不谈自由，理解这些系统也是很重要的，因为如果我们不理解它们，一般的趋势就是顺从权威，顺从那些理解系统的人或声称控制着系统的人，即便他们并不真正理解事情的本质。这就是我们看到这么多关于赛博战争的危言耸听言论的原因——因为那些似乎掌握着战争权力的人开始谈论技术，就好像他们理解技术似的。这些人现在总是谈论赛博战争，而他们当中没有一个人，哪怕一个，在谈论赛博空间的和平，或与缔造和平有关的任何事。他们总是在谈论战争，因为这就是他们的生意，他们努力控制技术和法律进程，以此作为促进他们自身利益的一种手段。所以，当我们失去对我们技术的控制时，这些人就希望为了他们的目标而使用技术，特别是用于战争。这会导致某些相当可怕的事情——正因如此，我认为我们会以震网病毒而告终——也有一些明白人在暗示，虽然美国发动了战争，但这类战术会以某种方式阻止战争。对于一个并没有积极入侵他国的国家来说，这似乎还能是一个合理的论据，但考虑到这里说的是一个正在同时进行多起侵略的国家，这就真叫人难以置信了。

注释

1．这场抗议发生在2008年4月6日，为声援遭到镇压的哈拉阿尔–寇布拉纺织工人的罢工。在这场罢工之前，“四月六日青年运动”已经在Facebook上形成了一个群组，他们号召埃及人民在开罗及其他地区发动抗议，以配合在哈拉阿尔爆发的工人运动。抗议并未如期举行，

Facebook群组的管理员埃斯拉·阿卜杜勒·法塔、艾哈迈德·拉希德和艾哈迈德·马赫尔等人遭到逮捕。马赫尔遭到刑讯，被要求交出他的Facebook密码。“四月六日青年运动”在2011年的埃及革命中继续发挥着作用。参见“Cairo Activists Use Facebook to Rattle Regime”，载于《连线》，2008年10月20日，http://www.wired.com/techbiz/startups/magazine/16-11/ff_facebookegypt?current-Page=all（访问于2012年10月23日）。

2．“How to Protest Intelligently”，作者匿名，于推翻穆巴拉克总统的18天起义开始时散发，http://www.itstime.it/Approfondimenti/EgyptianRevolutionManual.pdf；该文件被摘译为英文，以“Egyptian Activists’ Action Plan:Translated”为题发表于《大西洋月刊》，2011年1月27日，http://www.theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388（访问于2012年10月23日）。

3．环形监狱是英国哲学家杰里米·边沁（Jeremy Bentham）在1781年设计的一种监狱，这种设计使得一个监狱看守能在同一时刻秘密监视所有犯人。《论环形监狱》（*The Panopticon Writings*），杰里米·边沁著，米兰·博佐维奇（Miran Bozovic）编辑，Verso出版社1995年出版，在线版本：http://cartome.org/panopticon2.htm（访问于2012年10月22日）。

4．约翰内斯·古登堡（1398—1468）是一位德国铁匠，他发明的活字印刷机在历史上引发了重大的社会变革。印刷机的发明是与互联网的发明最相近的历史事件。

5．约翰·吉尔莫是最早的密码朋克之一，也是电子前哨基金的创始人和一位公民自由活动家。安迪引用的这段话首次出现在“First Nation in Cyberspace”中，载于《时代》周刊，1993年12月6日。参见约翰·吉尔莫的网站：http://www.toad.com/gnu（2012年10月22日）。

6．“专有技术是指任何为特定商业实体而开发的系统、工具或技术流程……由雇员提出并发展的想法一般被视为其雇主的知识产权，因而允许将这些想法也看作专有技术。”该定义出自wiseGeek：http://www.wisegeek.com/what-is-proprietary-technology.htm（访问于2012年10月22日）。

7．科里·多克托罗（Cory Doctorow）的“The coming war on general-

purpose computing”，载于boingboing，2012年1月10日（该文基于2011年12月提交给混沌俱乐部的一份主题报告）：http://boingboing.net/2012/01/10/lockdown.html（访问于2012年10月15日）。

8．震网病毒（Stuxnet）是一种极其复杂的计算机蠕虫病毒，它被公认由美国和以色列开发，用以攻击据说在伊朗核设施中所使用的西门子设备。震网病毒的一个概要，参见维基百科：http://en.wikipedia.org/wiki/Stuxnet；也可参见“WikiLeaks:US advised to sabotage Iran nuclear sites by German thinktank”，载于《卫报》，2011年1月18日，http://www.guardian.co.uk/world/2011/jan/18/wikileaks-us-embassy-cable-iran-nuclear。维基解密是震网攻击最早的报道者之一，该攻击导致了伊朗纳坦兹（Natanz）核设施的核事故，参见“Serious nuclear accident may lay behind Iranian nuke chief’s mystery resignation”，载于维基解密，2009年7月17日，http://wikileaks.org/wiki/Serious_nuclear_accident_may_lay_behind_Iranian_由维基解密披露的全球情报公司Stratfor的证据显示了以色列对该事件的参与，参见全球情报文档（The Global Intelligence Files），邮件号185945：http://wikileaks.org/gifiles/docs/ 185945_ re-al-pha-s3-g3-israel-iran-barak-hails-munitions-blast-in.html。（访问于2012年10月16日）

赛博空间的军事化

朱利安·阿桑奇：我看到现在存在一种赛博空间的军事化，即对赛博空间的军事占领。当你通过互联网通信时，当你使用移动电话通信时，移动电话现在已经跟互联网联结到了一起，军事情报组织正在拦截你的通信。这就像有一辆坦克停在你的卧室；这就像你跟你妻子用短信交流时，中间站着一个士兵。只要涉及我们的通信，我们现在都生活在军事管制之下，只是我们看不见这些“坦克”而已——但它们确实存在。在这个意义上，互联网，这个曾经被当作和平之地的空间，如今变成了一块军事空间。但是，互联网是我们的空间，因为我们通过它来彼此交流，与我们的家人交流。处于我们私生活内在核心的通信现在被转移到互联网上。所以，事实上，我们的私生活也进入了一块军事区域。就像床下有一个士兵，这就是公民生活的军事化。

雅各布·阿佩尔鲍姆：就在我来这儿之前，我被请去为华盛顿大学安全与隐私研究实验室的团队担任环太平洋大学网络防御竞赛的教练——我是直到最后一刻才被请去的。我们花了相当多的时间去完成一项网络战争竞赛，比赛在SPAWAR（美国空间与海战系统司令部）进行，这是美国海军的一个民用单位，能提供渗透测试[1]服务，包括防御性计算机黑客和进攻性计算机黑客。SPAWAR在比赛中担当红队，他们的任务是攻击其他参与者；每个队伍的任务是保护在比赛开始时交给他们的计算机系统，而他们事先对该系统毫无了解。你不知道你将要保护的是什么类型的系统，甚至在比赛开始时你都还不知道比赛的计分规则，所以你只能竭尽全力，期望成功. 。

朱利安·阿桑奇：你确定这真是个比赛？也许根本就不是比赛！

雅各布·阿佩尔鲍姆：不是，你只是得到了一堆计算机，然后你必须去保护它们，而对方入侵这些计算机并接管系统。这就像是现实中黑客大会上的夺旗赛（Capture the Flag）[2]的儿童版之类东西。这很有趣，因为这些家伙得到了很多工具，他们可以编写软件。

朱利安·阿桑奇：从美国海军的观点看，这个比赛的意义何在？

雅各布·阿佩尔鲍姆：嗯，从他们的观点来看，他们只是在资助这项赛事，因为他们想要培养未来的赛博战士。比如说，他们从中央情报局给你带来一个备忘录，因为他们在招募新兵。中央情报局里面有一个代号查理–查理（Charlie-Charlie）的家伙，他解释说，如果你想来参加比赛或者想加入中央情报局，这是一个在现实世界中找到工作的好机会。而且SPAWAR的人也在那儿，微软的人也在那儿招人。比赛的目的是训练所有参赛者，这些参赛团队，去继续参加全国大赛，去成为赢家，去“保卫祖国”，然后他们能够作为赛博战士去从事攻击性黑客行为，而不仅仅是网络防御者。我们在这次比赛中大概得了4000分，这比第二名、第三名和第四名得分的总和还要高。

朱利安·阿桑奇：干得漂亮。

雅各布·阿佩尔鲍姆：这不是我的功劳——我的励志格言是“没有最黑，只有更黑”，而且我也不觉得我特别擅长当教练——这些家伙真的很棒。但是，这件事的有趣之处在于一切都是在战争的框架中进行的，于是他们可以说：“嘿，我们想听到你的喊杀声。”就像在说：“对不起，怎么啦？”这就是当我们在系统保卫战中稍作休息时，比如在吃午餐时，他们在说的话。供给系统、战争、赛博战争以及思考方式的伟大，他们用这些术语来设计比赛中的一切。更有趣的是，除了我所在的团队，我发现很多参赛者都在苦苦挣扎，因为他们没有学过兵法——这更像是系统管理员锦标赛（Sysadmin Cup），他们只是在做系统防御——这让我感到很恶心。[3] 这种比赛令人感到非常怪异，因为这里到处是有军事背景的人，他们从战争的视角来看待问题，他们不是在教授技战术，他们关注的是对系统防御的修辞术，或是攻击其他系统，他们有太多的仗要打，他们真心想要激怒人们，激起人们的某种爱国狂热。他们不是在促进创造性思维或某种独立分析的框架；他们在推动一种机器齿轮式的心智，让人们跟从国家利益的命令行事。我之前从未有过这种体验。我感到很恶心，我团队中的大部分成员也很难消化这种思想，或认真对待它。

朱利安·阿桑奇：你认为这是美国海军的标准训练方式吗？他们现在把它运用到其他领域？这是美国网络作战司令部自上而下做出的决策，还是一种国际战略决策？

安迪·米勒–马贡：就像纳粹的童子兵营，他们在那里训练小孩。

雅各布·阿佩尔鲍姆：Sie konnen das sagen weil du bist Deutsche.（你

是德国人，所以你可以这么说。）其实并不是那样。美国海军介入只是因为美国政府资助了这项赛事。他们请我去当教练是因为他们那里需要能够做这种训练的人；而我同意了，是因为我喜欢这些参赛的家伙，这些本科生。但是随后发生的却是美国政府的确在试图向人们灌输这样的观念，他们想要从民族主义的视角来推动这些东西。这是一场非常非常奇怪的比赛：一方面，学会维护你的系统安全是一件好事，理解我们生活所依赖的基础设施也是一件好事；另一方面，他们并不想说服人们去理解它，他们只是在试图驱使他们陷入一种狂热，以此让他们对从事这类工作感到愉快。

安迪·米勒–马贡：不幸的是，美国对维护系统安全的兴趣其实非常有限，因为他们更想要脆弱的系统，这样就容易夺取控制权了。控制全球加密系统的尝试还没有达到美国在1998年左右最初推动它的地步，当时美国商务部负责国际贸易的副部长大卫·阿伦斯（David Aarons）访问世界各国，呼吁政府获取所有人的加密密码。[4] 但是，根据国际上所谓的《瓦森纳协定》（Wassenaar Arrangement），加密技术仍然被当作一种所谓军民两用技术来处理，终端产品形式的加密技术向很多国家的出口是受到法律限制的。[5] 在宣称某些国家及其行为邪恶的背景下，这听起来也许有些道理，但是，它显示出双重标准的一面，因为通信监控技术目前还没到受到出口限制。[6]

朱利安·阿桑奇：安迪，这几年你一直在设计加密电话。告诉我，现在所进行的针对电信的大规模监控都有什么类型？目前政府情报机构和大规模监控工业是怎么看待这项技术的现状的？

安迪·米勒–马贡：大规模存储意味着存储所有通信，所有语音通话，所有流量数据，所有用到短信服务的消费方式，包括互联网连接，在某些情况下，至少也要有电子邮件。如果你把军费预算与监控成本以及赛博战士的培训成本做一个比较，你会发现普通的武器系统会花费更多。赛博战士和大规模监控相比于一架战机来说是极为便宜的。一架战机大概会花掉你……

朱利安·阿桑奇：1个亿左右。

安迪·米勒–马贡：而且存储成本每年都在下降。实际上，我们在混沌计算机俱乐部做过一些估算：一年只花费大概3000万欧元，你就能得到一个存储系统，以良好的音质存储所有德国人的电话通话，而且还包

括管理费用，至于纯粹的存储成本大概只要800万欧元。[7]

朱利安·阿桑奇：而且，在南非还有像VASTech这样的公司，它们销售这种系统，每年要1000万美元。[8]“我们会拦截你的所有通话，我们会储存你所有被拦截的通话。”但是，最近几年发生了变化，从前是拦截一个国家到另一国家的所有通信，挑选出你想监听的特定人物，然后对其进行全面监听，现在则是永久性地拦截并存储一切信息。

安迪·米勒–马贡：从历史的角度稍微解释一下。过去，某个人会由于其外交身份、所效力的公司，由于涉嫌从事某事或与涉嫌从事某事的人有关而成为监听对象，然后你对他采取措施。现如今，他们认为这么做要高效得多：“我们将拦截一切信息，而且我们可以以后再来整理。”于是，他们就有了这些长期存储。可以把这个行业的工作分成两个主要部分——“战术”路径和“战略”路径。战术路径的意思是：“眼下，就在这个会谈上，我们需要在这里装个窃听器，我们需要让人把麦克风带进去，或把GSM（全球移动通信系统）监控系统部署在一辆车里，可以即时拦截人们的谈话，无须跟网络运营商交涉，无须提前获得搜查令之类的文件，不需要走法律程序，就这么干吧。”而战略则是默认执行的，就是记录一切事情，然后再利用分析系统进行整理。

朱利安·阿桑奇：所以，战略拦截就是把一个通信卫星正在转播的东西全部拿走，把一根光纤电缆上传播的东西全部拿走。

安迪·米勒–马贡：因为你永远不会知道一个人何时会成为嫌疑人。

雅各布·阿佩尔鲍姆：在美国，有一个称为国家安全局AT&T的案子，还有一个案子是Hepting诉AT&T。在加州的福尔松（Folsom），马克·克莱恩（Mark Klein），电信巨头AT&T公司的一位前技术员，曝光了美国国家安全局（NSA）一直在捕获所有数据，并要求AT&T向他们提交数据。他们所做的就是一股脑拿走所有数据，包括语音通话，所以，在马克·克莱恩曝光的那段时间，每当我在旧金山拿起电话或是连接互联网，我就知道美国国家安全局正在搜集所有这些数据，他们在美国的国土上对付美国的公民。[9]我相当肯定他们已经把拦截到的数据用在调查之中，他们一直在用这些手段对付美国人民。这引起了各种有趣的宪法争论，因为他们可以永久保留这些数据。

热雷米·齐默尔曼：我们还有Eagle系统这个例子，法国公司Amesys把这套系统卖给卡扎菲统治的利比亚，在一份商业文件上它被描述

为“全国性拦截机制”。这是一个你可以放在任何地方的大盒子，然后你就只管监听人民的通信吧。[10]

朱利安·阿桑奇：十年前，这还被视为一种幻想，被视为只有偏执狂才会相信的东西，但是大规模拦截的成本现在已经如此低廉，甚至像利比亚这样资源相对缺乏的国家也可以利用法国的技术来实施拦截。事实上，大多数国家已经在进行拦截了。

目前，我们看到很多国家对进出本国的所有通信进行战略拦截，然而，像是自动封锁银行账户，或自动部署警力，或仅针对特定群体拦截等诸如此类的后续行动，仍然处在转折点上。西门子正向情报机构推销一款自动实施行动的平台。于是，一旦移动拦截记录发现目标A正位于目标B的特定距离之内，目标A就能接收到一条提示邮件——一个关键词——然后就能触发一次行动。这就是正在发生的事。

注释

1 ．渗透测试（简称渗透）是一个安全工程术语，指的是一种对计算机系统或计算机网络进行的合法授权的攻击行为，用来评估系统或网络的安全性。安全研究员经常在黑客社群招募人员来作为非授权用户对系统的安全性进行渗透测试。

2 ．夺旗赛最初是一种户外游戏，通常包括两支队伍，每队都占据一片区域并守卫一面旗帜。游戏的目标是夺取另一队的旗帜，并返回自己的基地。在黑客大会上，黑客们进行计算机版本的夺旗赛，攻击和保卫计算机及网络。

3 ．系统管理员是在信息技术部中从事计算机系统或网络运维工作的人。雅各布的意思是，这种练习就是一场系统管理锦标赛。

4 . “Aarons says encryption protects privacy, commerce”，参见USIS华盛顿档案（USIS Washington File），1998年10月13日，http://www.fas.org/irp/news/1998/10/98101306_clt.html（访问于2012年10月21日）。

5 ．《瓦森纳协定》网站：http://www.wassenaar.org（访问于2012年10月21日）。

6 ．安迪指的是在20世纪90年代第一次密码战争中的各种发展。每当密码朋克开始把更强的密码工具当作自由软件传播开来，美国政府就采取行动去阻扰密码工具的有效使用。他们将密码术界定为一种军火，并限制其出口。他们引入故意破坏密码的竞争性技术以便执法机构能够解密信息，此外，他们还试图引进具有争议性的“密码托管”计划。在世纪之交后的短暂时期，这些尝试被广泛认为遭到了全面挫败。但是，现在“第二次密码战争”又打响了，那就是通过立法和技术手段来植入后门，或者排斥密码术的使用。

7 ．这里的样本计算基于德国在2010年发布的数据。当年德国有1964亿分钟的固定电话通信，用8 Kbps的语音编解码器进行数字化，总计11784 Pb的数据，加上额外的管理开销就是15 Pb。假设每1Pb的存储成本为50万美元，总共就是750万美元或600万欧元，再加上建立一个完善的数据中心的成本、处理数据的成本、网络和人力资源成本。即使把德国2010年共计1010亿分钟的移动通话也包括进来，也只是增加额外的50 Pb和1830万欧元，总价仍然低于一架像台风（价值9000万欧元）或F22（价值1.5亿美元）那样的战机。

8 ．更多VASTech的信息，参见窃听行星：http://buggedplanet.info/index.php?title=VASTECH（访问于2012年10月21日）。

9 ．美国国家安全局对美国境内进行的未经授权的监控是美国历史上后果最严重的一起大规模监控丑闻。1978年的美国《外国情报监视法案》（FISA）规定，美国情报机构对美国公民进行未经授权的监控是非法的。“9·11”时间之后，国安局得到乔治·W. 布什秘密行政命令的授权，开始进行大量违犯FISA的活动。布什政府声称，根据2001年美国国会通过的紧急立法，即《军事武力使用授权书》（AUMF）和《爱国者法案》（the PATRIOT ACT），他有权这么做。在2005年《纽约时报》曝光之前，国安局的未授权国内监控计划都是秘密进行的，其中还涉及与AT&T这样的私人公司的合作。参见“Bush Lets U.S. Spy on Callers Without Courts”，载于《纽约时报》，2005年12月16日，http://www.nytimes.com/2005/12/16/politics/16pro-gram.html?pagewanted=al。一位匿名的告发者联系《纽约时报》的记者，透露了这桩未授权监控计划的存在。2004年，在布什政府的要求下，《纽约时报》的执行编辑比尔·凯勒（Bill Keller）撤回这条新闻达一年，直到布什再次当选。2005年，《纽约时报》意识到这是一个潜在的类似五角大

楼文件事件的故事，于是赶在政府发出限令之前，刊登了这则报道。布什政府否认国安局的计划中有任何涉嫌违法的地方。司法部立即发起了一场对泄密源头的调查，牵连了25名联邦探员和5名公诉人。共和党高层要求根据间谍法对《纽约时报》提起诉讼。

随着《纽约时报》的曝光，其他告发者也投向媒体，逐渐揭示出一幅国安局最高层渎职枉法的详细图景。美国公民自由联盟（ACLU）和电子前哨基金（EFF）等诉求团体发起了大量集体诉讼。其中之一就是美国公民自由联盟诉国安局案，由于原告无法证实其本人遭到了监听，于是原告的地位遭到否认。在另一件Hepting诉AT&T的案子中，AT&T的一位告发者马克·克莱恩（Mark Klein）上庭做证，揭露出AT&T在美国境内监听计划中的参与程度。参见电子前哨基金网站上Hepting诉AT&T案的部分：https://www.eff.org/cases/hepting。

马克·克莱恩是Hepting诉AT&T案中的证人，他曾是AT&T的员工，在旧金山的福尔松（Folsom）工作，他对电子前哨基金就Hepting诉AT&T案所做的证词揭露了“641A房间”的存在，这是AT&T为国安局运营的一个战略性拦截设施。该设施能够访问光纤干线，包括互联网主干道数据流，能够监控通过这栋建筑物的所有互联网数据流，无论是国外的还是国内的。另一位国安局的告发者，威廉·宾尼（William Binney）估算出大概有20台这样的设施，全都安置在美国电信网络的关键节点上。克莱恩的证词提供了国安局监控性质的重要信息。这是一个“战略性拦截”的例子，即所有通过美国的互联网数据流都会被复制并永久储存。可以确定的是，美国国内的数据流也被拦截并储存，因为从工程学的观点看，处理如此规模的数据流是不可能筛选出哪些数据流符合FISA授权监控的。FISA的官方法律解释现在坚称，只有在国安局已经拦截并储存了国内通信，并可以在国安局的数据库中“访问”这些通信数据时，拦截才算发生，并且，只有到了这个阶段，才需要得到授权。美国公民应当假设他们的所有通信数据流（包括语音通话、SMS短信、电子邮件和网页浏览）都被监视并永久存储在国安局的数据中心。

2008年，为了应对窃听丑闻造成的大量诉讼，美国国会通过了对1978年《外国情报监视法案》的修正案，总统立即签署。这些法案授权了具有高度争议性的“追溯豁免”（retroactive immunity），以对抗对FISA违法的起诉。巴拉克·奥巴马议员在其总统竞选活动期间，将“透明性”作为其演讲口号之一，并承诺保护告发者。但当他2009年进入白宫后，他的司法部却继续着布什政府的政策，最终导致Hepting案的败诉

以及其他对AT&T的“追溯豁免”授权。虽然司法部对《纽约时报》最初报道来源的调查并没有找出那个告发者，但调查确实曝光了之后其他的告发者。其中之一就是托马斯·德雷克（Thomas Drake），他是国安局的一名前高级执行官，多年来他一直通过内部渠道向美国国会情报监督委员会投诉国安局“开拓者”（Trailblazer）计划中的腐败和浪费。但内部投诉遭到压制，虽然任何雇员都愿意走内部投诉渠道。在《纽约时报》报道之后，德雷克向《巴尔的摩太阳报》揭露了“开拓者”的故事。之后他遭到大陪审团调查，被指控为“国家敌人”，并以间谍罪遭到起诉。参见“The Secret Sharer”，载于纽约客，2011年5月23日，http://www. newyorker.com/reporting/2011/05/23/110523fa_fact_mayer?current-Page=all。

对德雷克的起诉在强有力的公众监督之下，于2011年6月遭到败诉，强迫德雷克进行认罪协商的企图也没有成功，之后司法部给以一项轻微的行为不当为其定罪。德雷克接受了一年的缓刑。

国安局的监控丑闻余波未平。在大赦组织等（Amnesty et.al）诉Clapper案中，美国公民自由联盟对2008年FIAS修正案提出违宪质疑。参见“FISA Amendment Act Challenge”，载于美国公民自由联盟网站，2012年9月24日，http://www.aclu.org/national-security/amnesty-et-al-v-clapper。

在Jewel诉国安局案中，电子前哨基金企图终结国安局的未授权监控活动。该案在奥巴马政府以国家安全机密为名义提出豁免要求后，于2009年遭到驳回。参见电子前哨基金网站上Jewel诉国安局案的页面：https://www.eff.org/cases/jewel。然而，2011年12月，第九巡回上诉法院允许重启该案。托马斯·德雷克和国安局的其他告发者威廉·宾尼和J. 寇克·威伯（J. Kirk Wiebe）也在Jewel诉国安局案中做证。在竞选演讲中强调政府透明性的奥巴马政府，以间谍罪起诉的告发者数量已超过之前政府的总和。（本条注释内所有链接均访问于2012年10月23日）

10 . 参见Eagle系统在窃听行星上的条目：http://buggedplanet.info/index.php?title=AMESYS#Strate-gic_.28.22Massive.22. 29_Appliances（访问于2012年10月22日）。

利用人的定律对抗全面监控

热雷米·齐默尔曼：现在这已经成为现实：技术能够实现对所有通信的全面监控。但硬币也有另一面，那就是我们能做些什么。我们可以承认，所谓战术监控的某些使用是合法的——在司法机关的监督下，调查人员需要用监控犯罪分子及其坏人和他们的手段来侦查网络。但问题是，这种司法监控的界限在哪儿，使用这些工具对公民进行控制的界限在哪儿。这是一个政策议题。当遇到这样的政策议题时，是对这些基础技术一窍不通的政客们在签署各种法律，但我认为，我们作为公民也要承担一种角色，不仅要对包括政客在内的人们解释这些技术的工作细节，还要参与到围绕这些技术使用的政治辩论中。我得知德国爆发了一场反对普遍数据保留的大规模运动，导致宪法法院推翻了数据保留方案。[1] 而欧盟现也正在进行一场关于修改数据保留指令的辩论。[2]

安迪·米勒–马贡：你在描述民主国家的理论，民主国家当然应该在法院的判决之内去甄别各处的坏人，监听他们的手机，并确保监听是以恰当的方式来进行的。这里的麻烦在于当局必须依法行事。如果他们不这样做，那他们又能得到什么好处？特别是通过这种战术路径，欧盟内的民主国家正在大规模购入能够使他们在法律之外行事的机器，因为这不需要法院的判决，他们只用按下开关就可以执行了，而且这种技术几乎不受控制。

朱利安·阿桑奇：但是，是否存在着两种对付国家大规模监控的途径：利用物理定律，以及利用人的定律？一种是利用物理定律，开发防范拦截的设备；另一种是制定民主控制的法律，以确保人们必须得到授权才能进行数据拦截，并确立某种监管问责机制。但是，战略拦截并不包括在内，它不可能受到监管的有效制约。战略拦截是不分青红皂白地拦截每个人的数据。我们必须记住，是统治集团的核心在从事这种监控。他们不可能有充分的政治意愿去曝光国家的间谍行为。而这种技术本身是如此复杂，在实践中又是被秘密地使用，所以不可能得到有效的民主监督。

安迪·米勒–马贡：或者你监听你自己的议会。

朱利安·阿桑奇：但也有很多借口——黑手党和外国情报机构——这些都是借口，让人们愿意接受建立这样一种体系。

雅各布·阿佩尔鲍姆：信息末日启示录的四骑士：儿童色情、恐怖主义、洗钱，以及禁毒战争。

朱利安·阿桑奇：一旦你建立了这种监控，既然它是如此复杂，既然它被设计成秘密进行的，那么它就不可能受到政策的监管了，难道不是这样吗？我认为除非是像冰岛这样的小国，除非存在革命性的条件，否则根本不可能通过立法和政策来控制大规模拦截。一切才刚开始呢。要绕开政治问责而实施拦截实在太便宜、太容易了。瑞典在2008年通过了一部拦截法案，即著名的FRA-lagen，这个法案意味着瑞典情报机构国防无线电局（FRA）在满足某些条件的情况下，可以合法地大规模拦截所有过境通信，把所获数据送往美国。[3] 一旦你设立了这样的拦截体系，一个执行拦截的秘密间谍机构，你怎么可能再贯彻这些附加条件呢？不可能。而且，已经出现的真实案例显示，FRA早已在各种场合中破坏了法律。许多国家完全将拦截行动置于法律管辖之外，根本就没有对此立法。所以，如果他们决定为了保护自己免遭起诉而通过修改法律来让这种行为合法化，就像瑞典的例子，那我们还要为此庆幸呢。而对多数国家来说，情况就是这样——大规模拦截正在发生，立法提案却在帮那些从事拦截的人擦屁股。

这种技术非常复杂。举个例子，在澳大利亚和英国针对全面拦截元数据的立法提案中，大多数人根本不懂元数据的价值，甚至不懂这个词本身是什么意思。[4] 拦截所有元数据意味着你必须建立一套系统以在物理上拦截所有数据，然后扔掉除元数据以外的所有东西。但是，这种系统是不可信的。除非有熟练的工程师得到批准去彻查所发生的事，不然没法判断这个系统实际上是否存在拦截和存储所有数据的行为。由于技术复杂性和保密政策的有害勾结，问题会变得越来越糟。真相被隐藏在复杂性中，被掩盖在各种秘密之中。不可问责性是内嵌于这种体系的，这是体系的一个特征。这是故意设计出来的危险。

热雷米·齐默尔曼：我不是在说政策途径就管用。我说的是一种民主体制如何发挥作用的理论，确实，即便在这种理论中你也能发现秘密机构，他们获准比一般的警察和调查人员走得更远。所以即使我们为一般的调查人员制定了适当的行为规范，也可能有其他人能够使用这些技术。但是，相对于对技术使用的监控而言，我们是否应该对它们的购买

和拥有进行管制，这也是一个实际问题。

朱利安·阿桑奇：他们购买的是能够拦截半个国家或城市的大规模监控设备。

热雷米·齐默尔曼：是的。就像核武器：你不能轻易出售核武器，而有些国家也许想制造这种武器但遇到了困难。当我们谈到武器系统时，这是一种受到管制的技术，管制的不是它的使用，而是它的制造。我觉得议题应该是，这种技术是否应该被当作战争手段。

雅各布·阿佩尔鲍姆：这要看情况。在叙利亚或利比亚这样的地方，监控设备就是一种武器，这毫无疑问——他们出于政治目的，利用它来针对目标人群。法国公司Amesys监控那些在英国使用法国设备的人，而这种监控在法国是违法的，他们却明知故犯。[5]

安迪·米勒–马贡：而且他们从前并未这么做，是吧？

雅各布·阿佩尔鲍姆：其实，Amesys就是因为他们自己的内部文件被抓住的，就是维基解密的间谍文档曝光的那些文件。[6] 如果我们要在武器的意义上来探讨这个问题，我们必须记住，这不是向一个国家出售一辆战车，而是向一个国家出售一辆战车、一个机修工和一个驾驶战车的团队，他们可以选择性地瞄准人群，然后向他们开火。

朱利安·阿桑奇：就像是出售一整套战车武器系统。

安迪·米勒–马贡：有意思的是，密码术曾经受到管制。《瓦森纳协定》是一部国际适用的协定，它意味着你不能向那些所谓的邪恶国家，或者出于某种原因而被认为是有问题的国家出口加密技术，这种技术有助于对抗监控技术。但是，如果你交易的是监控设备，就可以在国际上出售——协定中对此没有出口限制。我认为其中的原因在于，民主政府也是自私的，他们想要控制。而且，假如你在跟邪恶国家做生意，你把监控设备卖给他们去做坏事，那么你就能从中受益，因为你将知道他们在监听什么，他们在害怕什么，谁是对他们国家最具威胁的人，哪些是政府的反对派，谁在组织政治活动，等等。据此，你就能够预测未来会发生什么，你可以去赞助哪些行动，等等。国家之间正在发生的这些事让我们处在一种非常肮脏的交易中，这就是为什么监控系统不受管制的真相。

朱利安·阿桑奇：我想再探讨一下把大规模监控视为一种大规模杀伤性武器的这个类比。原子弹是可以制造出来的，这是一个物理事实，而一旦原子弹被制造出来，就会引发地缘政治的变化，许多人的命运将会发生不同的改变——有些人得到好处，其他人却被置于全面灾难的边缘。这就会出现一场要求控制局面的管制运动，到目前为止，这些控制使我们（除日本之外）免遭核战争。但同时，这也是因为这种武器的使用是很容易被发现的。

随着大规模监控在过去十年间变得越来越成熟，监控的成本也越来越低，我们现在正处在这样一个阶段，世界人口大约每25年翻一倍，而监控能力则每18月翻一倍。监控曲线压过了人口增长曲线。没有直接的办法可以逃脱。在我们现在所处的阶段，只需要1000万美元，你就能买到一个存储单元，它可以永久保存一个中等规模国家的大规模拦截数据。所以我怀疑我们对此是否有对等的回应。对全球民主和自由而言，这是一个真实的、巨大的威胁，我们需要一个回应，就像面对核战争时所做出的那种大规模回应，在我们还有能力这么做的时候，我们需要努力去控制局面。

安迪·米勒–马贡：我在利比亚看到了民主运动是如何奔向监控站的，他们得到了数据，可以用来证明西方企业在协助卡扎菲政权镇压运动，然而新政府完全接管了这些监管设施，现在这些设施又在全力运转了。[7]所以，尽管我的确同意技术控制是一个好主意，但我有点怀疑公民是否有兴趣对抗当权者的利益，因为无论是谁拥有这种可以窃听所有人手机的能力，他都会使用这种能力。这就像是库存率——从经济上说，如果你知道市场上正在发生什么，你就能赚得暴利。

朱利安·阿桑奇：有些国家会立法规定其主要电子间谍机构的监听对象，像美国的国家安全局，英国的政府通信总部，澳大利亚的国防部通信局等。他们也会修改立法以允许对经济情报的窃听。例如，澳大利亚和美国在谷物贸易上存在竞争，他们就窃听所有参与这项贸易的人员的通信。到目前为止这种窃听已经持续了很长时间，公认至少有十年了——但这是被允许的，因为无论如何人们都会这么干。最开始是窃听军火贸易，像洛克希德·马丁、雷神、诺斯罗普这样的军火公司也参与建造了大规模的拦截系统，因为这些集团都大量涉及权钱勾结。他们从朋友那里得到好处，建立符合国家安全标准的军火贸易信息拦截系统。但是，现在这种拦截适用于一切领域，几乎是一切国家可以从中获取经济利益的领域。

雅各布·阿佩尔鲍姆：2011年12月的混沌通信大会[8]上有人提出了一个很好的类比，他们说监控技术就像地雷，尤其是战术监控技术——当然也包括战略监控技术。我觉得这是非常可怕的。监控是可能的，但这并不意味着我们要无可避免地走上这条道路，也并不意味着我们必然会一往无前地奔向监控一切人的地步。

尽管有很多经济激励不利于我们。比如，曾有人对我解释说，挪威电话系统过去的工作方式像是在操作一个测速仪，测速的快慢取决于你的电话打得多远。但挪威电话公司不能合法地存储或分类保存通话的实际元数据，比如你的拨号，这源自第二次世界大战以来对隐私的忧虑。所以，以某种对隐私友好的方式建立同样的技术是可能的，而且也允许以基于市场的方式对经济做出贡献。然而，比如说在GSM移动技术上，我们就不可能取胜。此时此刻，这些系统建立的方式，不是从经营而是从基础架构的角度来看，它们不再给隐私留余地了，内容隐私不存在了。

朱利安·阿桑奇：一部移动电话就是一台可以打电话的追踪设备。

雅各布·阿佩尔鲍姆：确实如此。例如，如果第三世界中的所有人都遭到窃听，这个现实意味着什么？这意味着他们用来与世界其他地区进行联系的电话系统，可能就是他人用来搜集数据的间谍设备。

注释

1 . “German court orders stored telecoms data deletion”，载于BBC，2010年3月2日，http://news.bbc.co.uk/1/hi/world/europe/ 8545772. stm（访问于2012年10月22日）。

2 . 欧洲议会和理事会的2006/24/EC指令要求欧盟国家存储公民的电讯数据时间为6~24个月。该指令在德国法律中的施行被判定为违宪。2012年5月，欧盟委员会以不执行该指令为由将德国告上欧洲法院，参见欧盟委员的新闻发布：http://europa.eu/rapid/press-release_IP-12-530_en.htm（访问于2012年10月15日）。

3 . 参见“Sweden approves wiretapping law”，载于BBC，2008年6月19日，http://news.bbc.co.uk/1/hi/world/europe/ 7463333.stm，更多关于FRA-lagen的信息参见维基百科：http://en.wikipedia.org/wiki/FRA_law（访问于2012年10月10日）。

4 . 元数据是“关于数据的数据”。在本文讨论的背景中，元数据是指区别于电子通信“内容”的数据。元数据是信封而不是内容。对元数据的监控并不针对电子邮件的内容，却能提供围绕内容的所有信息，包括这封电子邮件的发件人和收件人、发件人的IP地址及真实位置、发件时间和每封邮件的日期，等等。但是，这里的关键是，拦截元数据的与拦截内容的是同一种技术。如果你授权某人监控你的元数据，那么其设备必然也能拦截你的通信内容。除此之外，大多数人没有意识到，“元数据归纳内容”，当所有的元数据都被搜集到一起，这就能提供关于一个人的通信的极其详尽的画面。

5 ．Amesys是Bull集团的一部分，曾是IBM的dehomag在向纳粹销售打卡系统方面的竞争者。参见埃德温·布莱克（Edwin Black）的《IBM与大屠杀》（*IBM and the Holocaust*，Crown Books, 2001）。更多关于卡扎菲使用Amesys监控设备监控在英国的利比亚人的信息，参见“Exclusive:How Gaddafi Spied on the Fathers of the New Libya”，载于OWNI.eu，2011年12月1日，http://owni.eu/2011/12/01/exclusive-how-gaddafi-spied-on-the-fathers-of-the-new-libya（访问于2012年10月22日）。

6 . 2011年12月，维基解密开始发布间谍文档（The Spy Files），曝光了大规模监控的规模，间谍文档可以在这里访问：http://wikileaks.org/the-spyfiles.html。

7 . 更多细节参见窃听行星：http://buggedplanet.info/index.php?title=LY。

8 . 混沌通信大会（The Chaos Communication Congress）是混沌计算机俱乐部组织的国际黑客年度聚会。

私人部门的间谍行为

热雷米·齐默尔曼：国家支持的监控确实是一个严重的问题，它在挑战所有民主体制的基本结构及其运作方式，但这里还有私人部门的监控和潜在的私人性质的大规模数据搜集。就看看Google吧。如果你是一个标准的Google用户，那Google就知道你在跟谁通信、你知道什么、你在研究什么，可能还有你的性取向，以及你的宗教和哲学信仰。

安迪·米勒–马贡：比你自己更了解你自己。

热雷米·齐默尔曼：比你妈妈，甚至也比你自己更了解你。Google知道你什么时候在线、什么时候下线。

安迪·米勒–马贡：你知道你两年前、三天前和四小时前在找些什么吗？你不知道吧，但Google就知道。

热雷米·齐默尔曼：实际上，我就是由于这些原因才不再使用Google的。

雅各布·阿佩尔鲍姆：这就像21世纪的“杀死电视”（Kill Your Television）[1]。这种拒绝使用Google的行为可以被视作一种可行的个人抗议，然而网络效应[2]的存在却不会让这种抗议真正产生多大效果。杀死你的电视，朋友。

热雷米·齐默尔曼：好吧，这不算是抗议，顶多是我个人看待事情的方式。

安迪·米勒–马贡：我看过一些精彩的电影，在里面，人们把他们的电视从三层楼丢了出去。

热雷米·齐默尔曼：这不只是国家支持的监控，而是隐私的问题，是第三方如何处理数据，以及人们认识到这些数据如何被利用的问题。我不用Facebook，所以对它不太了解。但是现在通过Facebook你可以看出用户的行为，他们很乐意交出任何类型的私人信息，你能指责人们没

有意识到隐私与公共领域之间的界限吗？几年前，在数字技术普及之前，人们的公共生活在于娱乐界、政治和新闻界，而现在每个人都通过点击“发布”按钮进入到公共生活领域。“发布”意味着让事情公开，意味着让全世界都可以接触到这些数据。而且，你会看到十来岁的小孩把他们喝醉了的照片或其他方面的信息发送出去，他们或许没有意识到，这意味着全世界都能看到这些，而且可能在很长的一段时间内都可以看到。Facebook就是靠模糊私人、朋友和公众的界限来做生意的。而且它还存储那些你认为只对你的朋友或者你爱的人有意义的数据。无论你以为你设置的资料的公开程度如何，当你在Facebook上点击“发布”时，你就首先把它交给了Facebook，然后他们再让其他Facebook的用户得到这些数据。

朱利安·阿桑奇：甚至连政府和公司的界限也被弄模糊了。看看过去十年中西方军事承包部门的扩张：十年前，有10家在册的主要承包商与世界上最大规模的间谍机构NSA合作：两年前，这个数字已经超过了1000家。所以，政府和私人部门之间的边界正在被抹掉。

热雷米·齐默尔曼：而且我们还可以说美国的间谍机构可以获得Google储存的所有数据。

朱利安·阿桑奇：他们确实是这么做的。

热雷米·齐默尔曼：还有Facebook的所有数据，所以从某种意义上说Facebook和Google是这些间谍机构的延伸。

朱利安·阿桑奇：雅克，你有一个Google的传讯是吧？就是发给Google的，要求它提交所有跟你的Google账户有关的信息？维基解密也接到过这样的传讯，是给我们在加州的域名注册商dynadot的，wikileaks.org就是在它那里注册的。针对维基解密，正在进行一个秘密的大陪审团调查，他们要求dynadot提交我们的财务记录、登录记录，诸如此类，dynadot全都交代了。[3]

雅各布·阿佩尔鲍姆：《华尔街日报》报道说Twitter、Google和Sonic.net这三家我正在使用或曾经使用过的服务商，每家都收到了一张2703（d）通知，这是很不寻常的秘密传票。[4]

朱利安·阿桑奇：属于《爱国者法案》的范围？

雅各布·阿佩尔鲍姆：不是，是《存储通信法案》。《华尔街日报》说每家服务商都声称政府会索要元数据，而政府声称他们有权在没有法院许可的情况下这么做。现在有个正在进行的法律案件，关于政府是否有权进行战术性保密，不只对公众保密，而且也要对法院记录保密。我和其他所有人一样，是读了《华尔街日报》才知道这回事的。

朱利安·阿桑奇：所以，在美国大陪审团调查维基解密的过程中，当政府索要用户记录时，Google对美国政府大拍马屁，这不是普通的传讯，而是一种特别的情报传讯。不过，2011年年初有报道称，Twitter也收到一些这样的传讯，来自同一个大陪审团。但是Twitter做出了抗争，要求解除禁言令并通知了所有被传讯的账户主人。我没有Twitter账户，所以并没有收到传讯，但是我的名字和布拉德利·曼宁的名字却出现在这些传讯上，作为需要被搜寻的信息。雅克，你有Twitter账户，所以Twitter收到了关于你的传讯。Google也收到了，但它们没有抗争，没有把消息公布出来。[5]

雅各布·阿佩尔鲍姆：据说确实如此，这是我在《华尔街日报》上读到的。我甚至不被允许引用它，除非扯上《华尔街日报》。

朱利安·阿桑奇：因为这些命令中也包括了禁言令？但这已经被认为是违宪的，不是吗？

雅各布·阿佩尔鲍姆：可能是吧。就Twitter的例子来说，我们提出暂停向政府披露数据的请求，我们解释政府一旦拿到这些数据就不会忘记，因此向政府披露这些数据将会造成无可弥补的伤害，然而，我们的请求被公开拒绝了。他们说：“好吧，是的，你的保留要求被拒绝了，Twitter必须披露这些数据。”我们还在走诉讼程序，特别是涉及判决的保密——我甚至不能谈及此事——就目前来看，法院说，如果你在互联网上自愿向第三方暴露信息，就别指望还有什么隐私，顺便一提，在互联网上每个人都是第三方。

朱利安·阿桑奇：甚至像Facebook或Twitter这种号称会保护隐私信息的组织。

雅各布·阿佩尔鲍姆：必然是这样。这就是国家与公司间界限的模糊。实际上最值得我们关注的事情是，NSA和Google基于美国国防安全的原因进行网络安全合作。

安迪·米勒–马贡：网络安全在这里可以指任何事情。这是个宽泛的术语。

雅各布·阿佩尔鲍姆：他们试图把所有活动都置于《信息自由法案》的要求之外，而且都要保密。此外，美国政府还坚持它有发出行政传票的权力，这比拿到搜查令的门槛要低。并且他们禁止第三方通知你，你无权争辩，因为这里直接涉案的是第三方，而第三方又没有宪法上的理由要去保护你的数据。

朱利安·阿桑奇：第三方可以是Twitter、Facebook或你的互联网服务提供商（ISP）。

雅各布·阿佩尔鲍姆：或者任何人。他们认为这是与银行隐私或拨号电话一样的一对一映射。你打电话的时候就自愿把号码暴露给了电话公司。你明白的，对吧？当你在打电话时，当你拨入这些号码时，你显然是在说，“我不指望还能保有这项隐私”。甚至跟机器的联系都没这么直白。人们不了解互联网如何工作——他们也不了解电话网络是如何工作的——但是就目前Twitter的案件来说，法院坚持规定事情就是这样。不幸的是，我无法对此进行真正的探讨，因为我实际上并不是生活在一个自由的国家，他们坚称本质上就是这么回事。[6]

想象一下，我们竟然把我们所有的个人数据拱手交给这些公司，而这些公司本质上变成了私人的秘密警察，这简直是疯了。而且就Facebook的案子来说，我们甚至享有“民主化”的监控。不像民主德国的斯塔西，他们付钱雇人当间谍，而我们则把这种间谍行为当作一种文化来奖赏——他们自己上钩了。人们报告朋友们的动向，“嘿，谁谁谁又订婚啦”；“哦，谁谁谁又分手啦”；“哦，我晓得现在该给谁打电话”。

安迪·米勒–马贡：有人根据欧盟数据保护法向Facebook施压，要求他们交出关于这些人的所有私人数据，结果是，单个用户的数据最少有350MB，最多的大概有800MB。[7]有意思的是根据这项法案，Facebook的数据库结构也被曝光了，包括你每次登录所用的IP地址、存储的每一件东西、每一次点击、每时每刻的所有活动，甚至还有你在一个页面停留的时间——所以他们能够猜测出你喜欢什么、不喜欢什么，等等。另外还曝光了这个数据库结构的主标识符，是“目标”（target）这个词。他们不把这些人叫作“订阅者”“用户”或者其他什么，他们管这些人叫“目标”，当然你可以说，“好吧，这是一个营销术语”。

朱利安·阿桑奇：但这些数据本质上都是私人的。

安迪·米勒–马贡：对，但是从军事角度看，它也可以是目标，或者从情报意义上讲，它就是目标。这仅仅取决于你在什么样的情景下利用这些数据。

朱利安·阿桑奇：对，这是最可怕的。

安迪·米勒–马贡：我认为这种曝光很有用。我们原来常常说对Facebook而言，这些用户实际上并不是客户。Facebook的用户实际上是它的产品，广告商才是它真正的客户。这是对这里所发生的事情最客气、最无害的解释了。

但是，问题在于你很难去指责一个符合国家法律规定的公司。这种行为被认为是正常的，如果公司不遵守国家的法律，你才能说它在犯罪。

所以你很难这么说。“嘿，人家是合法经营的。”你对此又能作何控诉？

雅各布·阿佩尔鲍姆：不对，这事我必须要争一争。如果你建造一套系统，它会记录一个人的一切信息，而且你知道你生活在一个法律允许政府强行搜集这些信息的国家，那么，或许你就不该建造这样的系统。在创建安全系统的时候，有两种不同的路径，一种是通过政策来保护隐私，一种是通过设计来保护隐私。当你企图以人们为目标时，而你也清楚你生活在一个可以公然监听人民的国家，就像Facebook把它的服务器放在卡扎菲治下的利比亚或者阿萨德治下的叙利亚，这完全是不负责任的。据我所知，至少这两年，被公开的国家安全信函没有一封是针对恐怖主义的。其中25万封是针对其他人，而非恐怖分子的。[8]所以我们看清了现实，事实就是这些公司在创建这些系统，它们选择为经济利益而出卖用户，它们是负有严重道德欠债的。这甚至跟技术无关，根本就不是技术问题，这就是经济问题。它们决定，更重要的是跟政府勾结起来，出卖它们的用户，侵犯用户的隐私，参与到这个控制系统中，而它们得到的回报是成为这种监控文化的一部分，这种控制文化的一部分——而非抗拒这种文化，所以它们成了其中的一分子，它们是共犯。

安迪·米勒–马贡：道德责任现在可算不上主要卖点，是吧？

注释

1 . “杀死电视”是指一种抗议大众传媒的方式，呼吁人们远离电视，参加社交活动。

2 . “网络效应”（network effect）是指一个人从事某种活动受从事此种活动的其他人的数量的影响。

3 ．更多关于大陪审团调查的信息，参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

4 ．据《华尔街日报》报道：“美国政府得到了一项具有争议的秘密法庭命令，强迫Google公司和小型互联网提供商Sonic.net公司交出维基解密志愿者雅各布·阿佩尔鲍姆的邮箱账号中的信息，根据《华尔街日报》所查证的文件……维基解密的案子成了对年初的法律解释的一个测试，当时Twitter抵制了法院要求交出维基解密支持者，包括阿佩尔鲍姆先生的账号记录的命令……该命令要求搜查‘互联网协议’或是人们登录他们账号的设备的IP地址。”一个IP地址就是分配给某个接入互联网的设备的唯一一组数字。这项命令同时也索要人们绑定这些账号所用的电子邮箱地址。这项命令被封印存档，但Twitter在法院成功赢得了通知这些被索要信息的用户的权利……《华尔街日报》查证了这些法令，它们索要的信息与要求Twitter提交的是同类信息。给Google秘密法令的日期是1月4日，这家搜索引擎巨头被要求交出阿佩尔鲍姆登录其gmail.com账户时的IP地址，以及自2009年11月1日起他与之联系的用户的电子邮件和IP地址。并不清楚Google是否抵制了这项命令或交出了文件。给Sonic的秘密法令的日期是4月15日，要求Sonic交出阿佩尔鲍姆先生邮箱账号中的同类信息，也是自2009年11月1日起。8月31日，法院同意解除Sonic的秘密指令的封印，并向阿佩尔鲍姆先生提供一份副本。“Secret orders target email”，载于《华尔街日报》，2011年10月9日，http://online.wsj.com/article/SB10001424052970203476804576613284007312问于2012年10月11日）。更多细节参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

5 . “WikiLeaks demands Google and Facebook unseal US subpoenas”，载于《卫报》，2011年1月8日，http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas（访问于2012年10月16日）。更多细节参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

6 . 参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

7 . 更多细节参见欧盟诉Facebook案网站：http://www.europe-v-facebook.org/EN/Data_Pool/data_pool.html（访问于2012年10月24日）。

8 . 国家安全信函（NSL）是美国当局发出的要求提供“非内容数据”或“元数据”的信函，数据包括金融交易记录、IP日志或电子邮件通讯录等。任何收到国家安全信函的人都必须按要求交出记录，否则就会面临起诉。发出一封国家安全信函并不需要得到法院的授权，它可以由联邦机构直接发出。因此，它很类似于所谓的“行政传票”——只提交行政部门索要的信息，而非司法监督之下的传票。基于此，国家安全信函被认为违犯了美国宪法第四修正案中对抵抗任意搜查和逮捕的保护。国家安全信函还包括了一种“禁言令成分”，这意味着收到国家安全信函的人不能向其他任何人谈论此事，否则就是犯罪。基于此，国家安全信函被认为是对第四修正案中对言论自由保护的违背。在Doe诉Gonzales案中，国家安全信函的禁言令被判定为违宪。法律修改为授权国家安全信函的接收人可以在法庭上质疑该信函，这样就满足了第二巡回法院的要求，如此一来，使用该信函就不再算是违宪。在2001年美国《爱国者法案》通过后，对国家安全信函的使用大量增加。国家安全信函的接收者一般都是服务提供商，比如互联网服务提供商或是金融机构。被搜查的记录通常为信函接收者的客户的信息。接收者不能通知客户他们的记录被搜查了。尽管接收者可以向法院质疑国家安全信函，但禁言令又阻碍了被搜查的目标得知有关国家安全信函的消息，这样也就阻碍了他们向法院提出质疑。为了说明这种抗辩多么困难，参见FBI副总法律顾问试图回答雅各布·阿佩尔鲍姆的问题时令人胆寒的视频，雅各布问道，“如果第三方被禁止谈论我已经成为你的目标这件事，那我又如何上告法官呢？”她回答道：“有时候，我们必须让事情处在控制之中。”：http://youtu.be/dTuxoLDnmJU（更多的背景资料参见Privacy SOS：http://privacysos.org/node/727）。

根据电子前哨基金的报道，“在所有因《爱国者法案》而扩大的危险的政府监控力量中，由《爱国者法案》第505条所扩大的美国法典第18编第2709节（18 U.S.C.#2709）之下的国家安全信函的权力是最可怕、最具侵略性的。这种信函作用于通信服务提供商，比如电话公司和ISP等，允许FBI向他们秘密索取有关普通美国公民私人通信和网上活动的数据，而这种行为不会受到任何有效的监督或事前司法审查。国家安

全信函的接收者受制于禁言令，不得向其同事、朋友或家人泄露该信函的存在，更不能向公众曝光。”参见：https://www.eff.org/issues/national-security-letters，亦可参见电子前哨基金搜集的、在《信息自由法案》（Freedom of Information Act）要求下发布的有关国家安全信函的文件：https://www.eff.org/issues/foia/07656JDB。（所有链接均访问于2012年10月23日）

赛博空间的军事化

热雷米·齐默尔曼：目前这个阶段所提出的一个问题是：解决办法是什么，无论对于个人用户还是作为一个整体社会？存在一些技术解决方案——分布式服务器，每个人都存储自己的数据、数据加密，每个人都只信任与自己接近的服务商，服务商为用户提供数据加密服务，诸如此类。我们已经讨论过这些政策选项。目前我不太确定的是，我们能否回答这个问题，两条路径中哪一条最好。我认为我们必须同时发展这两条路径。我们需要有人人可以理解、可以修改的自由软件，人人都可以检查它是如何运作的。我认为自由软件是一个自由的在线社会的基础之一，由此我们能够一直控制这套机器而不是被机器所控制。我们需要有更强大的密码术来确保，只要你愿意，你的数据只能被自己读取，其他任何人都无法读到。我们需要像Tor或加密电话这样的通信工具来保证你可以只跟你愿意交流的人通信。然而，国家的权力和某些公司的力量总是超过我们这些极客的力量，超越我们开发和传播这些技术的能力。在开发这些技术的同时，我们也许还需要让公民手中握有法律工具，以确保能控制——也许并不总是实时控制——这些技术的使用，如果这些技术的使用违反道德或侵犯了公民的隐私，法律工具会对其进行制裁。

朱利安·阿桑奇：我想来考察一下美国密码朋克和欧洲密码朋克视角的不同。美国宪法第二修正案保障人民持有武器的权利。最近我在看一个朋友在美国拍摄的一些关于持枪权的视频，在一家武器商店里有这样一句标语，“民主，装弹上膛”（Democracy, Locked and Loaded）。这就是你确保自己不被极权统治的方式——人民武装起来，如果人民真被激怒了，就会拿起武器，夺回权力。这种论据现在是否仍然有效其实是个很有意思的问题，因为过去三十年来武器类型发生了变化。再回头看一下这个宣言，现在我们可以说：编码——提供秘密的加密代码，让政府无法监听——就是武器。我们在20世纪90年代参加了这场战争，努力让每个人都可以使用密码术，而且几乎取得了胜利。[1]

雅各布·阿佩尔鲍姆：在西方取胜了。

朱利安·阿桑奇：在西方我们基本上取得了胜利，现在每个浏览器

都可以使用密码，尽管后面又有各种不同形式的破坏。[2]应当注意的是，你不能信任政府，以为他们宣称会执行这项政策，他们就真的去执行。我们必须提供我们自己控制的基本工具——加密工具，来运用我们的力量，因为只要密码管用，无论政府多么努力都无法直接破解你的通信。

雅各布·阿佩尔鲍姆：几乎所有现代权威的力量都来源于暴力或暴力的威胁。密码术必须得到人们的这种认可，即任何暴力都无法解决一道数学难题。

朱利安·阿桑奇：完全正确。

雅各布·阿佩尔鲍姆：这是最重要的关键。这并不意味着你不会受到刑讯，也不意味着他们不能在你的房子里装窃听器或通过某种形式搞破坏；这只是说，如果他们发现了一条加密短信，不管他们所做的一切是否听命于一个强权机构，这道数学题他们是解不出来的。然而，对于不懂技术的人来说，这件事并不是显而易见的，必须让人们明白这一点。如果我们可以解决所有这些数学题，那是另一回事了，但凡有人可以，那政府当然也可以解出这些数学题。

朱利安·阿桑奇：但这就是正在发生的现实，你可以提出很多即便是最强大的国家也解不出来的数学题，就好比你可以制造一颗原子弹。我认为这对于那些加州自由派和其他信奉类似“民主，装弹上膛”观念的人来说非常有吸引力。因为这是一种非常高智能的行事方式——一小群掌握密码术的人对抗世界上最强大国家的全部力量。

所以，宇宙的一种性质站在了隐私权这一边，因为有些加密算法是任何政府都永远无法破解的。还有一些算法，我们知道是连美国国家安全局都极难破解的。我们之所以能够这样断定，是因为这些算法被推荐给美军承包商用于保护美国军事通信中的最高机密，如果这些算法中有某种后门，那俄罗斯人或中国人很快就会发现，而这会使推荐这种不安全加密的决策人承担严重后果。所以，这种加密算法现在肯定是相当有效的，我们完全可以信任它们。不幸的是，你完全不能相信你运行这些加密算法的机器，所以这还是个问题。不过，这种问题不会出现在大规模监控中，只有那些已经被锁定为目标的人的计算机才会遇到这样的问题。除非你是一个安全专家，确保一台计算机的安全真是非常困难。但密码术可以对付大规模监控，而对全球文明构成威胁的正是大规模监控。个别监控并不构成这种威胁。

虽说如此，我还是认为，正如热雷米说的，我们正在与极其巨大的经济和政治力量对抗，可能的结果是，监控技术相对于人口数量的天然效率意味着我们将慢慢地终结于一种全球监控的极权主义社会——我所谓极权主义的意思是一种全面监控——也许最后还剩下一点儿可以自由生活的人，即那些懂得使用密码术来保卫自己对抗这种彻底的全面监控的人，那些完全与社会脱节、走进洞穴的新卢德派，或那些传统部落——那些不能享受现代经济效率的人，所以他们的行动能力也是非常有限的。

当然任何人都可以戒掉互联网，但这样他们就很难再有任何影响力。他们通过这种做法来让自己不受影响。使用手机也是同样的道理，你可以选择不用手机，但这就降低了你的影响力。这不是一种前进的方式。

热雷米·齐默尔曼：如果你从市场角度来看待这个问题，我相信存在一种对隐私的市场需求，只是这种需求几乎还尚未开发，所以或许某些公司会受到经济激励去为用户开发这种工具，让他们有独立的能力控制自己的数据和通信。这可能也是我们解决问题的一种途径。我不确定它能否单独起作用，但这是可能的，也许我们对此还不够了解。

朱利安·阿桑奇：密码术将无处不在。主要组织正在世界各地部署密码术，它正被逐渐推荐到联网的国家。如果你思考一下互联网上的通信路径——快速的跨国货币流动、跨国组织、组织内部的相互连接——所有这些通信都在不可信的通信渠道中流动，就像一个没有皮肤的组织。组织和国家之间的界线已经模糊了——世界上的每一个网络都在争夺优势地位——而且它们的通信流也被暴露给了机会主义者、竞争国家，等等。所以人们在互联网的顶层搭建新的网络——虚拟专用网（VPN）——并用密码术来保护他们的隐私。有一种产业权力基础在防止密码术遭到禁用。

你看看黑莓手机的例子，它有一套在黑莓手机网络中使用的内置加密系统。加拿大的捷讯移动科技公司（RIM）是黑莓手机的运营商，它可以解密普通用户的通信，而且至少在加拿大和英国有数据中心，所以英美情报共享联盟能够获得全世界黑莓手机之间的通信数据。但是，大型企业以某些更安全的方式来使用它。西方政府使用时情况还好，但当它蔓延到公司和个人用户，就引发了敌对的政治反应，就像我们在穆巴拉克统治的埃及所见到的那样。[3]

我认为对付即将来临的监控反乌托邦唯一有效的办法是你自己采取措施来保卫自己的隐私，因为那些有能力拦截一切的人并没有自我约束的动机。历史上与此相似的例子就是人们学会洗手的过程。这需要关于疾病的细菌理论的建立和普及，需要偏执狂来灌输这种理论——疾病会通过你手上看不见的细菌来传播，正如你也看不见大规模的拦截。一旦这种理论广为人知，肥皂制造商就会制造产品，人们就会消费肥皂来减轻他们的恐惧。给人们灌输这种恐惧是很有必要的，这样他们才能认识到问题，才能创造出足够的需求去解决问题。

在这个等式的另一边也存在一个问题，那就是程序声明自己是安全的，声明它们使用了密码术，但这些程序经常是欺诈程序，因为密码术很复杂，欺诈就隐藏在这种复杂性中。[4]

所以人们必须思考一下。唯一的问题是他们会从以下两条路径中的哪一条来思考。他们也许会想，“我需要注意自己的言谈，我需要遵纪守法”，在任何时间、任何交往中都要留心。或者他们会想，“我需要掌握一点儿技术，安装这些东西来保护自己，这样我才能自由地表达我的想法，才能自由地与朋友和我关心的人交谈”。如果人们不采取第二种行动，我们将会生活在一种全面的政治正确中，因为即使在与自己最亲密朋友交谈时，人们也要自我审查，也要把自己从世界政治的参与者中删除。

注释

1 . 参见前文注释中关于20世纪90年代第一次密码战争的内容。

2 . 朱利安提到的SSL/TLS是一种加密协议，现在已作为一种标准被包含在所有网页浏览器中，并用于安全浏览——例如，当浏览器用于访问网上银行时。

3 . 其中一个例子，参见“Blackberry, Twitter probed in London riots”，载于彭博，2011年8月9日，http://www.bloomberg. com/news/2011-08-09/blackberry-messages-probed-in-u-k-rioting-as-police-say-looting-organized.html（访问于2012年10月16日）。

4 . 举例而言，LulzSec团体的一名成员通过发布索尼客户的个人数据，曝光了索尼安全管理的漏洞。有关机构通过美国法院发出的命令，从代理网站HideMyAss.com上获取了他的真实身份后，此人遭到逮捕。

参见“Lulzsec hacker pleads guilty over Sony attack”，载于BBC，2012年10月15日，http://www.bbc.com/news/technol-ogy-19949624（访问于2012年10月15日）。

互联网与政治

热雷米·齐默尔曼：审视黑客的力量是一件很有意思的事——“黑客”一词最初的含义并非指一种犯罪。一个黑客就是一个技术狂热分子，喜欢钻研一项技术是如何运作的，让技术运作得更好而不是被技术所限制。我认为，当你五六岁时，试图拿起一把螺丝刀，打开一个装置去探究其内部构造，这就是黑客的行为了。黑客们出于很多原因去建设互联网，包括为了好玩，他们开发了互联网，并把互联网带给其他所有人。像Google和Facebook这样的公司却看中利用搜集用户的个人数据来建立商业模式的机会。但是，我们仍然能看到黑客们手中握有某种形式的权力。最近，我的主要兴趣在于，我们目睹着这些黑客夺取权力，甚至在政治舞台上夺取权力。在美国，SOPA（《禁止网络盗版法案》）和PIPA（《知识产权保护法案》）这种粗暴的版权立法基本上就是在给好莱坞授权，让他们可以命令任何互联网公司限制访问和进行互联网审查。[1]

朱利安·阿桑奇：还有金融封锁，就像维基解密所遭受的那样。[2]

热雷米·齐默尔曼：没错。那些金融公司对维基解密所做的正在变成对付邪恶盗版者的标准手法，这些盗版者摧毁了好莱坞的势力。而且，我们见证了来自互联网公民社会的强烈骚动，这并不仅仅发生在美国——如果仅仅是美国公民起来反抗SOPA和PIPA的话，这事不可能奏效。正是由于全世界所有人的参与，才使抗议取得了成功，而黑客们在其中居于核心地位，他们向其他人提供工具，帮助他们参与到公共讨论当中。

朱利安·阿桑奇：是他们促成了这场游说。

热雷米·齐默尔曼：像Tumblr或其他类似的网站，它们不是在首页上让你输入自己的手机号吗？之后你会收到回电，与美国国会取得联系，然后你就能开始跟国会里的人说：“瞧，这真是垃圾。”

雅各布·阿佩尔鲍姆：这是在利用互联网来保护互联网自身。

热雷米·齐默尔曼：我认为，我们黑客对自己开发的这些工具负有责任，并有义务向世界上其他人传播这些工具。我们或许正在见证这个开端，当我们集体行动时，这项义务可以何等高效地得到履行。如今，在欧盟也存在一场关于ACTA（《反假冒贸易协议》）的辩论——ACTA是一项跨国贸易条约，SOPA和PIPA就是以此为蓝本的。[3]我刚从欧洲议会回来，在议会上，作为个人代表，我们这些长着臭胡子的家伙在对一个议会委员会发号施令。我们给他们展示了欧洲议会议事规则中的一些条款——他们显然是第一次看到这些，还要告诉他们该如何行事，之后，我们以21：5的投票结果赢得了那场表决，把那个英国特派调查员赶到了小角落里。这只是反对ACTA的道路上一个小环节中的很小一部分，这个庞大的全球协议是背着我们设计出来的，就是为了规避民主。但是，作为公民，我们也许可以杀死这只怪兽——显然要利用互联网的工具，像邮件列表、维基、IRC聊天室，等等——而且我认为我们可能正在目睹一个时代——互联网的青年时代——的到来，以及社会如何利用互联网在更大的尺度上改变世界。我认为，我们黑客要利用我们的技术知识去指导人们，告诉他们，“你应该使用这些技术来掌控自己的隐私，而不是让Facebook或Google来掌控你”，这是至关重要的。把这两点结合起来，就能相对明白地阐述事情了。这可能有点儿乐观主义吧。

朱利安·阿桑奇：雅克，就互联网青年的政治激进化来说，特别是过去两年来，你一直在世界各地谈论Tor，对那些想要匿名、想要对自己的政府保持隐私的人们谈论Tor，那么，你一定也看到在许多不同的国家都发生了这类现象。这类现象有何重要意义呢？

雅各布·阿佩尔鲍姆：当然，我认为这是绝对重要的。我立马能想到的一个经典案例就是突尼斯。我在本·阿里政权垮台后去了突尼斯，我们在一个计算机科学班上讨论Tor，这个班里有一些大学里非常懂技术的人，其中有人举手问道：“但是，怎么对付那些坏人呢？”然后她不假思索地提到了信息末日启示录中的“四骑士”——洗钱、毒品、恐怖主义，以及儿童色情。“该拿那些坏人怎么办呢？”这四类事情总是被提出来，利用它们的幽灵来攻击隐私保护技术，因为我们显然必须对付这四类集团。于是，我向全班提问：“有人见过Ammar 404页面吗？”这是本·阿里政权在革命之前部署的一种审查页面，在革命进行时也用来禁止访问网页。房间里的每一个人，除了刚才提问的那人之外，都举起了手。然后，我看着那个发问的女孩，问道：“看看你身边的所有这些人，他们全都是你的同班同学。你真的相信，为了对付那些坏事而压迫这屋子

里的所有人，这是值得的吗？”然后她说：“实际上，我自己也举手了。”

从这个例子中我们还能学到非常重要的一点，那就是当人民能够设身处地时，他们才能明白真正的交易是怎么回事，然后事情就会发生戏剧性的逆转。而在全世界，每时每刻都发生着这样的事——虽然通常是稍后发生的，人们后知后觉地发现他们也可能使用这种技术，他们事后才意识到：“哦，对啊，事实证明并不只是坏人，因为如果我说了某些事情，如果当权的人不喜欢我不得不说的这些事情，那我就事实上就成了坏人。”于是，你看到了一场觉醒。

但要说这种情况仅仅发生在过去这几年，那就不对了。朱利安，我很抱歉要对你说这些，但是，正是你，你就是让我们这代人变得激进的原因之一。要这么算起来的话，我大概算是第三代密码朋克。你和拉尔夫·维曼（Ralf Weinmann）对rubberhose文件系统所做的工作就是激励我去开发加密系统的一部分原因。M.A.I.D是我设计的一套加密文件系统，用来反击英国的常规调查权这类事情，英国政府基本上采取消极的管制来解决密码术的问题，这样他们才能拿走你的秘密。[4] 当然，在朱利安的例子中，他们开发这套工具是因为压迫性的政权会折磨人们以获取密码，所以你们必须能够交出不同的密码，以应付他们的折磨。我的加密文件系统M.A.I.D是为这样一种法制体系而设计的，在这种体系下，被告有权保持沉默，但如果强迫他们，他们也能够在不破坏机密的情况下证明他们所说的是真话。当我看到朱利安的工作时，我意识到你能够利用技术赋予普通人以改变世界的力量。回到更遥远的老密码朋克的邮件列表时代，蒂姆·梅（Tim May）是列表的创始成员之一，正是由于阅读了朱利安在密码朋克列表中发布的那些旧帖子，整整一代人开始变得更激进，因为这些人意识到，他们不再是原子式的孤立的个体，他们可以花时间去编写软件，而这些软件能够赋予百万人以权力.。[5]

这些还都只是意想不到的后果，毕竟创建Google的人当初也并没有想把Google建成史上最大的监控器。但是，事实上，这个监控器就这么建成了，而且只要人们开始认识到这一点，他们就会发出那些国家安全信函，是吧？

热雷米·齐默尔曼：我觉得你刚才所说的话中，有三点是很关键的。

雅各布·阿佩尔鲍姆：只有三点？

热雷米·齐默尔曼：其他也很重要。

安迪·米勒–马贡：好吧，我们也许还能加上第四点，试一试？

雅各布·阿佩尔鲍姆：你还不知道我说的是哪三点呢。

热雷米·齐默尔曼：我发现这三点是纠缠在一起的。其一是数字技术时代的极权统治及其掌权者。在本·阿里政权的例子中，当然也在当今许多政权中，统治者都能决定人们能知道什么，或与什么人交往。这是相当惊人的权力，人们应当抵抗这种权力：而互联网，一种自由的互联网，就是能够拿来抵抗这种权力的工具。其二是要制造工具并改良技术，那种能够绕开审查之类麻烦事的技术，但更重要的是，要制造那种能作为基础设施的工具，这些基础设施可以帮助我们推翻独裁者。其三是政治叙事，你经常提到的信息末日启示录“四骑士”，就是政客们每天都在媒体上利用的借口，说什么“难道让恐怖主义把我们都害死吗？因此，我们需要《爱国者法案》”或“到处都是儿童色情”“互联网上到处都是小纳粹（pedo-Nazis），因此我们需要审查”。

雅各布·阿佩尔鲍姆：小纳粹？

热雷米·齐默尔曼：对，小纳粹，pedo-nazi.com已经保留下来了。“艺术家正在走向灭亡，不会再有电影了，因此我们必须给好莱坞授权，让他们来审查互联网。”诸如此类的说法。我认为，互联网在此再度成为一种工具，一剂对付政治叙事的解药。政治叙事依赖于煽情造势和媒体的时间尺度，这种时间尺度极其短暂，一则信息的出现与消失都在24小时之内，然后就被新的信息所取代。通过互联网，我感觉我们是在建造所谓的互联网时间。因为伟大的互联网永不遗忘，我们可以日复一日、年复一年地建立卷宗，我们还能做研究、能做分析。这就是我们在过去三年中对ACTA所做的事情。维基解密又一次鼓舞了我们，因为ACTA的初版就是维基解密在2008年披露的。[6]

朱利安·阿桑奇：对，是我们揭露了此事。

热雷米·齐默尔曼：之后我们自己又披露了两个版本。这三年来一共有五个版本，这让我们可以逐段逐行地进行研究，说明这条是做什么的，那条又是哪个行业的要求，法律专家和技术专家也加入到这项工作当中，我们形成了一套不同于官方政治叙事的版本。官方的说法总是，“哦，我们需要ACTA来拯救文化、拯救孩子、打击假药”云云。现

在我们利用互联网时间，通过仔细的分析，艰苦的工作，以及团结人们参与其中来形成我们自己的政治叙事。

朱利安·阿桑奇：真是这样，而我认为这种对ACTA的观点赢得了公众。

热雷米·齐默尔曼：目前为止，干得不错。

朱利安·阿桑奇：我认为这是一种看待此事的历史观点，但在幕后，最初由美国版权行业搞出来的这个所谓的《反假冒贸易协议》，实际上已经用在相当多的双边贸易协议中，他们企图创建一种新的国际制度，来规定何种出版是合法或非法的，并且创建阻止人们从事各种出版活动的机制。这套制度以美国的DMCA体系（《数字千年版权法案》）的一种更严厉的版本为标准，在这个体系下，如果你给某人发出一封信，要求他从互联网上删除某些东西，他们就必须删除，虽然会给他们两周左右的时间让他们提出抗议，但是，由于对互联网服务提供商而言处理这种抗议太费钱了，于是他们就会立即删掉这些东西，然后让作者或上传者自己去尝试捍卫自己的权利。这种做法在美国造成了严重的影响，导致大量内容被删除。山达基教[1]（Scientology）被证实利用这条规定，从YouTube上删除了数以千计的视频。[7]

所以，我们可以假设ACTA已经在欧洲议会中被踢出局了，至少在这轮议程中，实际上是出局了。尽管如此，ACTA似乎仍然在取得重大进展——在我们的民主辩论中，ACTA已经臭名昭著，我们赢得了话语权，但在幕后，秘密的双边协定已建立起来，并达到了同样的目的，这颠覆了民主议程。例如，维基解密获取并发布了新的欧盟—印度自由贸易协定，其中很大一部分就是ACTA的内容。[8]其他很多协定和法案也出现了这种情况。他们把ACTA的标题和内容分离开来，再把内容分割成更小的部分，让这些部分像蠕虫病毒一样渗透到各种事务当中，以各种双边协定的形式渗透到国际制度当中。这样一来，在公众眼中，你们取得了民主的胜利，但这只是一种表面上的胜利，而在表面之下，情况一如既往。从这种情况中，我看得出政策或立法改革并没有奏效，尽管你也不能把主动权交给对手，那样他们就会加速进程。所以，重要的是，要以各种方式来进行检查，就像检查ACTA那样。这样才能延缓事情的发展速度。然而，就算我们在议会中取得了立法的胜利，还是无法阻止台面下的活动。

雅各布·阿佩尔鲍姆：我觉得有一件事必须要特别指出，Tor的创始人之一罗杰·丁格勒戴（Roger　Dingledine）在某种程度上可以算是我的导师，关于审查规避和匿名在线的问题，他启发我进行了很多思考。就我们现在所讨论的话题，比如说，防火墙取得的成功不仅仅是技术上的，也是社会性的，因为如果你想要从技术上对抗防火墙，那么理解这项技术的背景也是相当重要的。反抗ACTA的人们也在使用技术，这些技术能帮助他们进行反抗，但是，事实上，更重要的是去理解普通人的日常事务，而不是那些复杂的技术术语。真正要紧的是，让人们切实参与到这种讨论中来，参与到改革中来，在他们还有权力这么做的时候。而且，事实上，正是事情的这种人性方面，才是最重要的。维基解密发布的文件推动了信息共享，这是重要的，但是那些获得了重要信息并把信息传播出去的人也是至关重要的。因为，这里存在一种说法，说我们大多数人都生活在一种民主制度中，说我们是自由的，据说政府是通过人们的同意来统治他们的。如果我们每一个人都对正在发生的事情有所了解，并且发现所发生的事情跟我们所同意的并不是一回事，那么，在没有取得被统治者同意的情况下，事情就不会这样轻易地进行下去了，立法也不会那么顺利就得到通过了。

热雷米·齐默尔曼：就是要增加做出错误决策的那些人的政治成本，只有把互联网掌握在自己手中，我们才可以通过一个自由的互联网来促成这种集体行动。

雅各布·阿佩尔鲍姆：但在没有互联网的时候你也能这么做，因为在历史上，在前互联网时代，我们也有自由结社，只是那种方式在经济上更昂贵，遇到的困难也更多，而这实际上就是点对点（P2P）[9]运动如此重要的原因。

安迪·米勒–马贡：第四点，我认为是去中心化（decentralized）系统的基础建构维度，这是一个核心要点。这种基础建构也需要掌握在人民手中，因为现在已经有集中化（centralized）的云计算了。[10]

朱利安·阿桑奇：Facebook是完全集中化的，Twitter是完全集中化的，Google也是完全集中化的。它们都位于美国，都可能受制于那些掌握强制性权力的人。就像维基解密发布电报门之后，审查就开始了，亚马逊把我们的网站从它的服务器上删除了。[11]

安迪·米勒–马贡：而且，云计算还给公司提供了一种经济激励，把

数据交给所谓的国际数据中心处理，这是一种更便宜的数据处理方式，但那些数据中心其实都是由美国企业运营的，这就意味着把数据置于美国的司法管辖区内，就像支付公司的情况那样。

朱利安·阿桑奇：向云计算转移数据的趋势相当令人担忧。太多的服务器集群都位于同一区域，因为这样更便于对环境进行标准化控制，也便于对支付系统进行标准化处理。这是一种更有竞争力的技术，把服务器集中到同一地区总比把它们分散到各地要便宜。除了流媒体电影之外，互联网上的绝大多数通信都是发生在服务器之间的，所以如果你把服务器放得更近，那自然会更便宜。最终，我们就得到这些通信服务器的巨型蜂巢。举例来说，Google有必要把它的服务器放置在大型内容提供商附近，或者反过来，内容提供商有必要把服务器放在Google附近，因为Google要对这些页面建立索引以供搜索。所以，在美国就存在这种巨型建筑，这些建筑被各家公司的服务器填满。这些地方也是国安局的大规模拦截搜集点。没有这种集中化，互联网也可以存在——这在技术上是可能的，但集中化更有效率，仅此而已。在经济竞争中，集中化的方式取得了胜利。

安迪·米勒–马贡：但是，从基础建构的观点来理解这件事也非常重要，集中化的基础设施就意味着中央控制，这让权力滥用变得非常容易。这就像你家隔壁的小型超市倒闭了，取而代之的是集中零售。

朱利安·阿桑奇：而且还会像Safeway（美国大型连锁超市）那样，成为巨型的跨国零售巨头。

安迪·米勒–马贡：对，基础设施的集中化就和购物领域中发生的故事一样。保持一种去中心化的基础设施建设模式非常重要。当我还在ICANN（互联网名称与数字地址分配机构，负责分配和管理互联网上的域名）任职时，我从文斯·瑟夫（Vince Cerf）那里学到了一些东西。他是TCP/IP协议这项互联网基础通信协议的发明者之一，他过去总是说：“你知道吗，关于政府的一件好事是，它们从来不是单数，它们总是复数。”所以，即使在政府之间，也存在想要拥有自己的去中心化的政治力量的人，即使在政府内部，也存在相互斗争的不同派别。这最终将我们从“老大哥”的手中解救出来，因为太多人想当“老大哥”了，所以他们会自相残杀。

朱利安·阿桑奇：我不这么看，安迪。我认为那种国内精英相互竞争的局面很多年以前是存在的，如今他们都团结起来了，脱离了各自的

民众。

安迪·米勒–马贡：这点你说得对，他们是团结起来了。但我们也有机会能保住我们自己的身份，虽然我也不确定这是否能救我们一命。我们必须坚持建造我们自己的基础设施，如果我们想要反对这种监控状态，想要反对“老大哥”的话，这就是我们需要知道的最重要的事情。我们必须研究这到底是什么，是否存在一种集权国家的联络，说：“嘿，如果我们团结起来，我们就能得到更多。”我们还需要知道我们在其中所承担的角色，那就是要保持去中心化，拥有我们自己的基础设施，而不是依赖于云计算或其他垃圾，我们必须使用自己能掌握的东西。

朱利安·阿桑奇：但是我们可能遇到这样一种技术统治。如果，使用Twitter比开办你自己的Twitter更容易；如果，使用Facebook比使用DIASPORA [12]或其他替代品更容易；如果，云计算更便宜，那么这些技术和服务就会取得统治地位。说什么我们应该开启自己的本地服务器，这类说法毫无意义，因为这些本地服务器根本就没有竞争力，而且也只有一小群人会使用它们。我们需要的是更好的东西，而不是说我们应该有一个穷人版的Facebook，还指望人们去使用它。

安迪·米勒–马贡：好了，现在回到天主教会，我们就要回到只有一个大型图书发行机构的时代了，因为亚马逊现在试图完全控制电子书供应链，所以我们必须保住我们自己的出版和发行能力。这可能有点儿多虑了，但我们已经看到，如果这些公司或它们在其司法管辖区内所依赖的政府机构不希望看到某些事情发生，他们可能做出什么事。我还认为，下一步的必要措施是我们要有自己的货币，这样就算他们反对我们支持像维基解密这样的项目，我们也能用我们自己的方式去做成事情，而不必依赖那种会将所有数据发往某个司法管辖区的中央基础设施。

热雷米·齐默尔曼：我同意安迪的看法。我认为这种基础建构非常重要，这是我们为之奋斗的一切的核心。但这也是一个我们有义务向公众传达的信息。因为，作为黑客，作为每天都在建设互联网并与之打交道的技术人员，我们懂得其中的道理。也许这也是赢得年青一代人支持和理解的一种方式。我认为正因如此，版权战争才变得如此重要，因为通过自1999年Napster开始的P2P技术，通过在个人之间共享文件，人们才开始理解……

朱利安·阿桑奇：你是个罪犯。

热雷米·齐默尔曼：不，这是在建立更好的文化。

朱利安·阿桑奇：不对，你就是个罪犯。

热雷米·齐默尔曼：他们是这么编故事的，但是如果你为自己建立起了更好的文化，那么每个人都会使用Napster[13]。

安迪·米勒–马贡：人类物种的历史和人类文化的历史就是对思想的复制、修改和完善的历史，如果你把这叫作偷窃，那你就跟那些愤世嫉俗的家伙是一伙的了。

热雷米·齐默尔曼：就是这样，完全正确！文化就意味着共享。

朱利安·阿桑奇：好吧，西方从20世纪50年代开始就有了所谓的工业文化。我们的文化已经成了一种工业产品。

热雷米·齐默尔曼：我们这是被钓鱼了，因为这家伙正在充当魔鬼的辩护士，他还乐此不疲。

雅各布·阿佩尔鲍姆：我不跟你们争，这明显就是瞎扯淡。

热雷米·齐默尔曼：就是瞎扯淡啊。在那种政治叙事中，他们管这叫偷窃，我想明确我的观点，那就是每一个在1999年使用Napster的人都成了音乐爱好者，而后他们会去音乐会，并告诉每一个人，“你真该去听听那些人的音乐，你真该去听听那场音乐会”，等等。于是，对于P2P技术如何实现了去中心化的建构，人们就有了实践经验。实际上，Napster在当时还是有点儿集中化的，但它为一种去中心化建构的理念埋下了种子。每个人都有了一个具体的实例来显示去中心化建构如何有益于社会，而这种建构对于文化共享的促进也同样作用于知识的共享。当我们在讨论绕开审查或揭穿政治叙事以建立更好的民主体制和更好的社会时，我们讨论的就是知识共享。

所以，我们有了通过去中心化服务和个人间的共享来改善事情的实例，而反例就像扮演魔鬼辩护士的朱利安那样，在一个行业出现时，他就会说：“哦，这是在偷窃，这是在杀死大家，杀死演员，杀死好莱坞，杀死电影，杀死小猫和一切。”他们赢得了过去的战斗，而现在我们可能即将取得ACTA战役的胜利。我重申我不同意魔鬼的辩护士朱利安玩的这套把戏。ACTA是迄今为止规避民主的最大的一个实例，他们

坐在议会和国际机构面前，坐在公众舆论面前，又通过幕后交易来强行实施不可接受的措施。如果我们能设法解决掉这个问题，那么我们就树立了一个先例，我们就取得了推动一个积极议程的机会，就是说，“ACTA已完，现在我们来做一些真正有益于公众的事吧”。我们正在努力推动这件事，欧洲议会中的一些议员现在也明白了，当人们分享东西时，当人们不为牟利而分享文件的时候，他们不应该被送进监狱，他们不应该遭受处罚。我认为，如果我们能做到这一点，我们就为全世界树立了一个强有力的案例，知识的共享、信息的共享，会让事情变得更好，我们必须推动而不是打击这种共享，想要破坏我们以去中心化的方式共享信息和知识的能力的任何企图，无论这种企图是来自立法机构、独裁者，还是公司，我们都必须反对。我认为我们能够创造这种势头。

朱利安·阿桑奇：那美国关于PIPA和SOPA的辩论又如何呢？这是美国国会提出的新法案，代表工业界的利益去建立金融制裁和互联网封锁。

雅各布·阿佩尔鲍姆：这是专门针对维基解密和与维基解密相关或类似于维基解密的东西的。

朱利安·阿桑奇：在国会，他们指出，针对我们的金融封锁是一项很有效的措施。[14]

热雷米·齐默尔曼：他们还想把这种措施提供给好莱坞。

朱利安·阿桑奇：所以我们形成了一场反对封锁的大规模社群运动，最终，Google、维基百科，还有其他一大帮人都加入了这场运动。但是我不会说：“好啊，真了不起，我们赢得了这场战斗。”这件事令我相当惊恐，因为，Google突然意识到自己并不仅仅是一个销售商，而是一个政治大玩家，而且他们感觉到了自己有超越国会的巨大的、可怕的权力。

热雷米·齐默尔曼：Google只是反对SOPA和PIPA联盟中的一小部分。

雅各布·阿佩尔鲍姆：是的，但是等一下，我觉得Tumblr对此事的影响就超过了Google。

安迪·米勒–马贡：Tumblr和维基百科，以及成千上万的个人行动，那些小到你从来没有听说过的个人行动，造成了这种影响力。数以千计的行动同时发生，朝着同一个方向，这里我们又看到去中心化的政治行动。我们见证的正是这种去中心化的政治运动。Google也许是你所注意到的这些活动中最大的参与者。

朱利安·阿桑奇：好吧，这是国会说的，他们注意到了这一点。

雅各布·阿佩尔鲍姆：对于热雷米之前说过的一个问题，我想再谈一点儿看法，因为你基本上是在推崇一种政治先锋队的观念。我不认为你打算那么做，但你就是那么说了，所以在这里我只是想稍微打断你一下，因为P2P运动是明确反对一个政治先锋队的。这种观念是，我们都是对等的，我们可以彼此分享，我们可以提供不同的服务或提供不同的功能。我认为罗斯·安德森（Ross Anderson）是这个运动的思想先驱，有一次，他对我说：“我在50年前就加入了P2P运动。”他解释说，他想确保我们永远不要消灭印刷机。因为当我们开始有了集中化的服务，例如我们开始集中控制信息系统，我们其实就开始消灭印刷机了。《大英百科全书》不再印刷了，他们只出版CD。如果你没有一台可以读取这些CD的通用计算机，你就无法获取这些知识。现在，这个《大英百科全书》的例子已经无关紧要了，因为我们有了维基百科，我们还有其他许多资源。但是，我认为整个社会还没有做好这种准备。

安迪·米勒–马贡：我不确定维基百科作为一种资源是否已经足够好。我不相信单个网页，除非我可以自己重写它。

雅各布·阿佩尔鲍姆：但是《大英百科全书》也是一样。这是众多来源中的一种，重要的是对信息的核实。我想表达的意思是，我们不应该鼓吹这种先锋的观念，这个观念是非常危险的。

朱利安·阿桑奇：等等，为什么危险？我差不多就算是一个先锋。这有什么问题？

热雷米·齐默尔曼：我不是在讨论这些先锋，我所说的是我们手中握有新的工具。我们现在提到了印刷机。另一位思想家邦雅曼·巴亚尔（Benjamin Bayart），他是我的一个朋友，可能在法语世界之外不太知名，他曾说：“印刷机教会人们如何阅读，互联网教会人们如何写作。”[15] 这是很新鲜的东西，这是一种新的能力，让每个人都可以去写作和表达自己。

安迪·米勒–马贡：是的，但现在过滤也在变得更加重要了。

热雷米·齐默尔曼：那当然，因为人人都能发言，多数人说的都是废话。我猜，就像学者兼活动家拉里·莱斯格（Larry Lessig）[16]或其他很多老师会告诉你的，我们教人们怎样写作，但当学生们交上他们的作业时，99%都是废话，尽管如此，我们还是要教他们怎样写作。所以，人们当然会在互联网上胡说八道，这是显而易见的。但是，随着时间的推移，你能够运用这种能力在公共场合表达自己的意见，这让你逐渐能够以自己的方式来建构你的话语，越来越有效地参与到复杂的讨论中。而我们现在讨论的所有现象，都是围绕工程上的复杂性建立的，我们需要把这种复杂性分解成一个个较小的部分，这样我们才能理解问题，才能心平气和地进行讨论。这与政治先锋队无关，而是关于通过将这种政治制度掌握在我们自己手中，将这种能力用于发表我们自己意见的问题；我们要分享我们的思想，要参与知识的共享，但不必像过去那样，为了表达自己的意见而成为某个党派、某个传媒公司，或是无论什么集中化组织的成员。

注释

1．SOPA指的是《禁止网络盗版法案》，PIPA指的是《知识产权保护法案》。两项法案都是美国在2012年年初提出的，并受到全世界的瞩目。两个法案都是以美国唱片工业协会这类团体为代表的内容产业提出的公开透明的立法诉求表达，他们希望在全球范围内以最严厉的标准强制执行知识产权法，以应对文化产品在互联网上的免费分发。两个法案都要求授予美国执法机构强大且广泛的互联网审查权，并威胁要“打破互联网”。两个法案都激怒了主要的国际在线社区，并激起那些以自由和开放的互联网为自己切身利益的行业从业者的强烈反抗。

2012年年初，Reddit、维基百科和其他上千个网站关闭了它们的服务器，以示对这两项法案的抗议，这煽动起对公众代表的强烈舆论压力。其他像Google这样的在线服务提供商，也促成了请愿。作为回应，两项法案都被搁置，等待重新考虑和讨论它们是否代表了对网络知识产权问题的最佳解决办法。这一事件被视为互联网行业在国会的游说力量的第一次重大展示。

2．参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

3．ACTA指的是《反假冒贸易协议》。这是一项多年来处于秘密谈判中的国际多边条约，由美国和日本主导，其中部分内容确定了保护知识产权的新的严格义务。

ACTA的初步草案在2008年被泄露给维基解密后得到公开，这激起了自由文化活动家和网上诉求群广泛的强烈抗议。参见维基解密上ACTA的章节：http://wikileaks.org/wiki/Category:ACTA。

2011年年初，由维基解密向La Quadrature Du Net分享的美国外交电报显示，ACTA秘密谈判的明确目的是为创造极端的知识产品执法规则提供快速通道，这些内容将在之后强加给那些被排除在协议之外的贫穷国家。参见“WikiLeaks Cables Shine Light on ACTA History”，载于La Quadrature Du Net，2011年2月3日，http://www.laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history（访问于2012年10月23日）。2012年7月，由La Quadrature Du Net和热雷米·齐默尔曼领导的一场游说活动在欧洲议会中挫败了ACTA。

4．M.A.I.D.，即（相互）确保信息毁灭，是“一个提供时间敏感型遥控密钥托管和带可选遇险编码的可证明验证的框架。当超过既定用户设置的时间阈值后，它能自动毁灭加密密钥”：https://www.noisebridge.net/wiki/M.A.I.D。像《2000年调查权规范法案》（RIPA，Regulation of Investigatory Powers Act of 2000）这样的立法使得英国成为一个相当敌视密码术的政权。在RIPA之下，根据警员的要求，个人有解密数据或提交密码的义务，这里不必有司法监督，而拒绝服从则会导致刑事指控。在随后的审判中，如果被告声称忘记了密码，则负有辩方举证责任。为了避免被判有罪，被告必须提供他忘记了密码的证据。这点遭到法律界的批判，被认为是实行了有罪推定。相比之下，虽然就同一情况，美国也发生了大量诉讼，而且情势也不理想，但在类似的情形中，对第一和第四修正案的引援也取得了大量成功。参见司法部2011年11月4日发布的报告“Freedom from Suspicion,Surveillance Reform for a Digital Age”：http://www.justice.org.uk/resources.php/305/freedom-from-suspicion。

更多关于Rubberhose文件系统的信息参见赛利特·德雷福斯：“The Idiot Savants’ Guide to Rubberhose”，http://marutuk-ku.org/current/src/doc/maruguide/t1.html。（所有链接均访问于2012年10月24日）

5 . 一份老密码朋克邮件列表的文档可以在此处下载：http://cryptome.org/cpunks/cpunks-92-98.zip。蒂姆·梅（Tim May）是密码朋克邮件列表的创始成员之一。参见他的Cyphernomicon，这是有关密码朋克历史和哲学的一份常见问题答卷：http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html。（两条链接均访问于2012年10月24日）

6 . “Proposed US ACTA plurilateral intellectual property trade agreement (2007)”，载于维基解密，2008年5月22日，http://wikileaks.org/wiki/Proposed_US_ACTA_multi-lateral_intell-ectual_property_trade_agree-ment_%282007%29（访问于2012年10月21日）。

7 . “Massive Takedown of Anti-Scientology Videos on YouTube”，载于电子前哨基金，2008年9月5日，https://www.eff.org/deep-links/2008/09/massive-takedown-anti-scientology-videos-youtube（访问于2012年10月16日）。

8 . “EU-India Free Trade Agreement draft,24 Feb 2009”，载于维基解密，2009年6月23日，http://wikileaks.org/wiki/EU-India_Free_Trade_Agreement_draft,_24_Feb_2009（访问于2012年10月21日）。

9 . 点对点或P2P指的是一种每台计算机都对其他所有计算机既充当客户端又充当服务器的网络，其中，每台计算机都可以发送并接收信息，这种网络允许内容的快速共享，包括音乐、视频、文件或任何类型的数字信息。

10 . 云计算指的是这样一种情形，由一台计算机来执行很多传统的功能，诸如数据储存（包括各种应用的用户数据）、托管并运行软件，以及为软件的运行分配处理能力，这些功能都在本机之外，由远程的“云端”服务器执行，“云端”通常由云计算服务公司通过互联网来提供。再也不需要一台全功能的个人计算机了，用户需要的只是一台能够连接上网的设备，剩余的服务都可以通过互联网获取。“云端”的隐喻掩盖了这样一个事实，那就是用户的所有数据和元数据实际上都存放在某个数据中心的某台远程计算机上，这个数据中心多半是由像亚马逊这样的大公司控制，虽然用户对数据不再拥有完全的控制，但其他某些人却有这种控制权。

11 ．参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

12 ．DIASPORA是一种社交网络，它允许每个安装了DIASPORA软件的用户都能充当自己的服务器，从而保留对他们自己数据的控制权。这创造了一种能够替代Facebook的符合隐私标准的产品，并且是非营利和用户所有的：http://diasporaproject.org。

13 ．最初的Napster（1999—2001年）是提供音乐分享的P2P服务的先驱。它曾广为流行，但是很快就因与美国唱片工业协会的版权官司而倒闭了。在破产之后，Napster这个名字被卖给另外一家销售音乐营利的网上商店。

14 ．参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

15 ．邦雅曼·巴亚尔是法国数据网络（French Data Network）的总裁，这是法国现存最老的ISP，也是网络中立性和自由软件的呼吁者。参见他的维基百科条目（法语）：http://fr.wikipedia.org/wiki/Benjamin_Bayart（访问于2012年10月15日）。

16 . 拉里·莱斯格是美国学者和活动家，他关于版权和自由文化的观点最为知名，他的博客：http://lessig.tumblr.com（访问于2012年10月15日）。

[1] 山达基教，又称科学神教或科学教，新兴宗教之一，由美国科幻小说作家罗恩·贺伯特（L. Ron Hubbard）于1952年创立。——编者注

互联网与经济

朱利安·阿桑奇：我想来考察下三种基本自由。我采访真主党的首领哈桑·纳斯鲁拉（Hassan Nasrallah）时……

雅各布·阿佩尔鲍姆：该死的无人机在哪儿？这里在搞什么？ [1]

朱利安·阿桑奇：好吧好吧，他也相当于遭到了软禁，毕竟他不能离开自己的藏身地。

雅各布·阿佩尔鲍姆：我不认为我可以做出这种比较。请别再做这种比较了。

朱利安·阿桑奇：真主党是否具备组成国家的要素是有争议的——它真变成了个国家吗？美国大使馆电报中提到一些事情，真主党在黎巴嫩南部发展了自己的光纤网络。[1] 所以，一个国家由三种基本要素组成——对特定区域内武装力量的控制，对通信基础设施的控制，以及对金融基础设施的控制。另外，我们也可以把这些看作三种基本自由。迁徙的自由，物理上的行动自由——我们从一个地方旅行到另一个地方而不被武力所限制。我们可以想一下思想的自由与通信的自由，后者内在于思想自由当中——如果你的公开讲话受到威胁，唯一能保障你的通信权利的办法就是秘密通信。最后，经济交易的自由，就像通信自由一样，也与经济交易的隐私结合在一起。那么，让我们谈一下这些从20世纪90年代开始就在密码朋克中酝酿的观点，密码朋克一直在努力提供这至关重要的第三种自由，即经济交易的自由。

热雷米·齐默尔曼：但是为什么你只需要这三种自由？我们在欧盟基本权利宪章中都有更多自由。

朱利安·阿桑奇：隐私权变得很重要。从一种社群主义的观点看，为了自由交流和自由思考，你需要隐私权；在经济交易中，你也需要隐私权。所以，我认为有很多派生的自由，但我刚才所说的这三种自由是最基本的，其他的自由都从中派生而来。

热雷米·齐默尔曼：好吧，对于基本自由，我们是有法律定义的。

朱利安·阿桑奇：但是，我读过欧盟宪章，我可以告诉你其中达成的所谓共识可以说是一团糟。

热雷米·齐默尔曼：是的，好吧，说客们还想把知识产权塞进欧盟宪章呢。

朱利安·阿桑奇：各种神经病。

安迪·米勒–马贡：我认为有一点我们肯定都同意，那就是现在的货币体系，这个货币交换的经济基础设施，真是糟透了。任何拥有eBay账户的人都会深表同意，因为PayPal、VISA和万事达的所作所为完全就是把人们推入实质性的垄断境地。从维基解密的电报中也可以看到这类很有意思的事，据说，俄罗斯政府想跟VISA和万事达协商出一种办法，让身处俄罗斯境内的本国公民的支付在俄罗斯境内得到处理，而VISA和万事达当然是拒绝的。[2]

朱利安·阿桑奇：对，美国使馆和VISA联合起来就有足够的力量去阻碍俄罗斯控制其本国的支付卡系统。

安迪·米勒–马贡：那就是说，就算是俄罗斯公民在俄罗斯商店中进行的支付也要通过美国的数据中心来处理。所以美国政府拥有对这些俄罗斯事务的司法管辖能力，或者至少可以察觉。

朱利安·阿桑奇：对，所以如果普京要出门买杯可乐，华盛顿下一秒就能知道。

安迪·米勒–马贡：对，那当然，这真是一种相当令人不满的状况。无论我喜欢还是讨厌美国，让一个中心来存储所有支付信息，这本身就是件非常危险的事，因为这个中心对这些数据可以为所欲为。

雅各布·阿佩尔鲍姆：密码朋克认为最根本的一点是基本建构实际上定义了政治局面，所以，如果你有一个集中化的建构，即便由世界上最好的人来控制它，它也会吸引混蛋，而那些混蛋会利用他们的权力去做那些设计者本来没想去做的事。重点是要知道这关系到金钱。

朱利安·阿桑奇：就像是沙特阿拉伯的油井，所谓的石油诅咒。

雅各布·阿佩尔鲍姆：无论从哪个角度看，我们都能发现，这跟金融体系的本质有关，即使人们怀有最好的动机，这都无关紧要。基本建构反映了真相。这也是互联网在通信方面的真相。所谓的合法拦截系统，其实只是让监控人民听起来没那么刺耳的说法……

朱利安·阿桑奇：一种委婉修辞，合法拦截。

雅各布·阿佩尔鲍姆：确实，就像合法谋杀。

安迪·米勒–马贡：或者合法刑讯。

雅各布·阿佩尔鲍姆：你听说过美国总统奥巴马对美国公民发动的无人机攻击吗？他在也门杀了安瓦尔·奥拉基16岁的儿子，他们管这叫合法谋杀或定点清除。[3] 所谓的合法拦截也是这么回事——只要你给任何事情冠上合法之名，顷刻间，国家所做的事情就都变成合理合法的了。但实际上这就是国家的基本建构允许他们这么做，这是法律的建构，也是技术的建构，同样也是金融体系的建构。

密码朋克想做的就是创造让人们可以真正自由地相互帮助的体系，消除干涉的可能。就像乔姆币（Chaumian），这是根据电子现金（eCash，一种完全匿名的电子货币）的创始人大卫·乔姆（David Chaum）的技术规范设计出的电子货币，尽管你还是可以争辩说它们比实际所需的更集中化。这种想法是创造出匿名货币，对抗VISA或万事达那种可追踪的货币。乔姆币虽然围绕一个中心权威而建立，但使用了大卫·乔姆发明的密码协议来保证交易的匿名性。[4]

朱利安·阿桑奇：所以说，本质上是没有序列号的电子现金。

雅各布·阿佩尔鲍姆：或者允许你创建序列号，但这些序列号只是为了检验货币真伪，而一定不能允许你知道朱利安付钱给了安迪，或金额是多少。

热雷米·齐默尔曼：这其实是在数码世界重新创造现金。

朱利安·阿桑奇：创造电子现金绝对是一笔大买卖，因为控制交易媒介是组成国家的三种基本要素之一，就像刚刚我谈到真主党时所说的。如果你夺走了国家对经济交易手段的垄断控制，你也就夺走了这个国家的三种基本要素之一。如果把国家看作一个黑手党，那么国家就是

个收保护费的，竭尽所能盘剥百姓。控制货币流动对国家税收来说很重要，但同样重要的还有控制人们的行动——激励一件事，打击另一件事，或完全禁止某项活动、某个组织或组织间的交易。拿针对维基解密的异乎寻常的金融封锁为例，封锁维基解密并不是自由市场所做的决定，因为这并非自由市场——政府管制使特定的金融玩家成为国王而排斥其他市场参与者。一个能同时影响政府管制和银行规则的精英团体已经对经济自由造成了严重侵害。[5]

安迪·米勒–马贡：说起来伤心，对现在的电子世界来说，这是个无解的问题。全世界的大部分信用卡支付被两家信用卡公司掌控着，它们都使用位于美国的电子基础设施来处理清算，这意味着在美国的司法管辖权内可以获取这些数据。像PayPal这样的公司，也处于美国司法管辖之下，遵守美国的政策，却可以封锁德国网上零售商对古巴雪茄的销售，或是阻止来自美国司法管辖区之外的对维基解密的支付。这意味着美国政府可以访问这些数据，并有权对全世界范围内的支付实施管制。

尽管美国公民也许会争辩，这是能够用钱买到的最好的民主，但对欧洲公民来说，这没多少价值可言。

朱利安·阿桑奇：在传统的世界中，我们还享有一定程度的行动自由，虽然在某些情况下也不算太多。

雅各布·阿佩尔鲍姆：你确定，朱利安？我觉得你的行动自由就是一个经典的例子，显示我们的行动有多自由。

朱利安·阿桑奇：好吧，这不算什么，英国宣称他们每年将十万人置于我这样的处境。[6]所以我认为这在一定程度上是附带的。

雅各布·阿佩尔鲍姆：这就是为什么我的祖国的开创者们要对那些英国来的人开枪。这就是我们对英国人开枪的原因。到今天还是这种情况！还存在这种暴政。

热雷米·齐默尔曼：我们别扯上个人好恶。

安迪·米勒–马贡：你的国家，美国，目前正在做的事情就是把监狱私有化，并跟这些运营前美国政府监狱的私营公司签约，保障90%的监押率。[7]好啊，这算什么？这是资本主义所能做的最荒唐的事。

朱利安·阿桑奇：美国监狱里关的人甚至比当年苏联监狱里关的还要多。

雅各布·阿佩尔鲍姆：这是个谬误，因为我反对某件错事，你就暗示我也是某件同样错误的事情的一部分。我不是在暗示说美国就是完美的。我觉得美国在很多方面的确很了不起，特别是那些跟国父们的豪言壮语有关的方面。

朱利安·阿桑奇：国父们的豪言壮语在过去十年里已经烟消云散了。

雅各布·阿佩尔鲍姆：我们不能忘记，很多关于国父言论的观念都是神话，我们需要警惕这种偶像崇拜，当然，这也很自然。当我说到英国的暴政、说到朱利安自身的处境时，我的意思是说，这其实是一种文化。这种文化有它的社会基础，而且，可以说社会发挥了非常重要的作用。这是技术难以克服的方面。而插手金融问题是最危险的事。这就是创造另一种电子货币比特币（Bitcoin）的人必须要匿名的原因。你不会想成为第一个真正成功发明电子货币的人。[8]

朱利安·阿桑奇：搞出电子黄金（e-gold）的那些家伙最后都在美国被起诉了。[9]

雅各布·阿佩尔鲍姆：实在太让人泄气了。

朱利安·阿桑奇：我想回到那三种基本自由的问题：通信的自由，行动的自由和经济交易的自由。我们可以看看正在互联网化的全球社会，人身行动的自由基本上没有变化，但通信的自由在很多方面都得到了极大增强。我们现在可以与更多的人交流，但另一方面通信自由也被严重侵害，因为人们不再有隐私，我们的通信可能被监听和保存，而且结果可能被用来对付我们自己。另外，人与人之间基本的物理交流也在衰退。

安迪·米勒–马贡：隐私还是可以有的，但这要付出代价。

朱利安·阿桑奇：我们的经济交易也因同一原因而遭到损害。在传统的经济交易中，谁知道这些？是看见你走进市场的那些人。而现在，又是谁了解你的经济交易？比如你用VISA卡从隔壁邻居那里买了什么，在传统市场社会中你也可以这么做，而且几乎是完全私密的，而现

在是谁知道这些？

雅各布·阿佩尔鲍姆：所有人。

朱利安·阿桑奇：所有人都知道。西方的主要大国之间共享数据，他们都知道，而且把知道的永久保存下来。

安迪·米勒–马贡：朱利安，你说的是不错，但我不太肯定你是否真的可以把通信自由和经济交易自由区分开来，因为互联网是我们今日社会的基础设施，是我们的经济、文化、政治，一切交易的基础。

雅各布·阿佩尔鲍姆：特别是行动的自由。

安迪·米勒–马贡：无论通信的基础建构是什么，货币都是比特。这只是对互联网的一种利用。如果经济体系的基础是电子基础设施，那么电子基础设施的建构就反映了货币如何流动、如何受到控制、如何被集中化，等等。也许目前互联网还不能被当作一切事物的基础设施，但经济逻辑却在说，“在互联网上做事更便宜”。从前，银行和信用卡公司的ATM（自动柜员机）是接入X.25协议网络 [10] 的，那是十多二十年前的一种独立网络，现在一切都基于TCP/IP协议了，因为这样更便宜。所以技术的基本建构正在成为一个关键问题，因为它将影响其他一切领域，这才是我们需要反思的。也就是说，如果我们想要一种去中心式的经济形式来处理我们的支付，我们就要将基础设施掌握在我们自己手里。

雅各布·阿佩尔鲍姆：比特币本质上就是一种电子货币。

安迪·米勒–马贡：还没有通货膨胀。

雅各布·阿佩尔鲍姆：比特币更倾向一种去中心化的处理方式，因此，不必像美联储那样，你有一帮来自世界各地的人，大家一起决定现实是什么，他们的汇率是多少。

朱利安·阿桑奇：而且还有促进实现它的一些计算机程序。

雅各布·阿佩尔鲍姆：我想用一种非技术性的方式来解释一下。这是一种更像商品而非货币的电子货币，因为人们能决定多少欧元可以兑换一个比特币。所以，这样看来它有点儿像黄金，而且对比特币的所谓挖矿会产生一项成本，你需要在计算机上通过一种搜索来找出一枚比特

币，这个想法的重点是这里存在一种运算的复杂度，它与货币的价值有关。所以不用技术术语来说明，它就是提供了一种方式，让我可以向朱利安发送货币，而朱利安可以确认这个支付，这些安迪都不能干涉或阻止。尽管这里也存在一些问题——它其实并不是真正匿名的货币，在我看来这是最糟的。

朱利安·阿桑奇：比特币是一个有趣的混血儿，因为账户持有人是完全有隐私的，你也可以随意创建一个账户，但是整个比特币经济中的交易是完全公开的。这就是它的运作方式，它需要用这种方式来获得所有人对一项已发生交易的同意，现在，付款账户的余额减少了，目标账户的余额相应地增加了。这是运转一种分布式货币的少数方法之一，它不需要一个中央服务器，而中央服务器是强力控制的有利目标。比特币的真正创新之处在于它的分配方式，以及这种分配方式背后的算法，在比特币的银行网络中，如果你愿意，你不用信任其中的任何一个特定部分。相反，这种信任是分散的。而且它并不通过法律、监管或审计来强制实施，而是依靠密码的运算难度来执行的，网络中的每个部分都必须证明它在做它所声明的事。所以，诚实的比特币“银行业”的运行是建立在这个系统的基本建构之上的。运算被转换成比特币银行每个分支的电费，所以我们可以根据电费为欺诈分配一个成本。为实施一项欺诈所需要做的工作的电费被设定为高于其所得的经济收益。这是非常有创意的，并不是因为我们从前没发现这些想法（这些想法至少20年前就在理论中出现了），而是在于比特币掌握好了平衡，还增加了一个非常好的创意来实现交易中的一种真正的全球化同意，哪怕我们假设很多银行都喜欢欺诈，而且任何人都可以实施欺诈。

当然，就像其他所有货币那样，你必须用其他东西来购买这种货币，通过工作，或用另一种货币来交换比特币，有很多外汇团体都在干这事儿。这里还存在其他一些限制。结算时间大约需要十分钟——在货币交割和另一方确认所发生的交易获得了全球化同意之间，需要一个十分钟的运算过程。这完全就像现金，所以现金所遇到的一切偷盗问题它也会遇到：一旦你得到一个比特币，你就确实得到了支付，这项确认既不能被取消，也不能被银行撤回。强制性的力量联系切断了它们之间的关联。另一方面，你必须保管好现金。我觉得这是比特币最大的问题。但是在其顶端建立额外的层次也是相当容易的，可以在你存储比特币的地方搭建托管服务器，这个服务器可以专门设计，以确保安全并增加防止盗窃的设施。

雅各布·阿佩尔鲍姆：相当有趣，如果比特币的发明者强制要求使用Tor浏览器，那你就不必再创建一个账户了，你可以创建一些密码标识符，即便有长期标识符可以识别出你。如果一切以Tor为核心来设计，那就有可能实现地址的匿名，你可以把你所有的交易关联在一起。

热雷米·齐默尔曼：不必陷入技术讨论我们也能同意，比特币是一个卓越的概念，但还有些瑕疵。它带有一种通货紧缩的本性，因为来自比特币的钱是易于消失的。所以它不可能具备长期效用，但它给出了可以改进的概念。所以现在的比特币可能只是0.7或0.8版本的。

雅各布·阿佩尔鲍姆：就像大卫·乔姆重新发明的电子货币。[11]

安迪·米勒–马贡：我认为，比特币是过去十年来引进一种数字货币的最成功的尝试。

朱利安·阿桑奇：他们达到了适当的平衡。我认为比特币会继续存在。它是一种高效的货币，你可以在十秒钟内创建一个账户，然后转账，这里不存在手续费，除了网费和几分钟的电费。相比于其他几乎所有形式的换汇，它都具有极高的竞争力。我认为比特币会流行起来。可以看一下几起比特币盗窃之后发生了什么，以及2011年夏天负面的追踪报道，这些事件导致比特币对美元的汇率跌到了1：3。[12]后来比特币对美元又逐步回升到了1：12。它并没有马上爬升或反弹，而是沿着一个平缓的曲线爬升的，这显示出对这种货币存在一种广泛的需求。我怀疑大部分需求来自小额毒品交易、邮购大麻，诸如此类。[13]某些互联网服务提供商已经开始使用比特币了，特别是来自那些不太容易得到信用卡服务的地区，比如前苏联地区。

如果比特币继续发展，就可能遭到打压。你不可能摆脱比特币，因为密码保护着比特币的运行免受强制力量的简单攻击，但兑换比特币的某些外汇交易服务却非常容易成为打击目标。另一方面，这些交易可以在世界上任何地方进行，在没有更多的外汇兑换之前，一笔换汇必须经过相当多的司法管辖区，而且黑市也有它自己的兑换逻辑。我觉得比特币要去引导这个游戏，让它被互联网服务提供商和服务行业所采用，让你可以用比特币来购买Facebook这种平台上的小游戏，因为这非常高效，而且一旦各种行业都采用了比特币，他们就会形成一个游说团体来阻止对比特币的封杀。这有点儿像密码术得到采用的过程：密码术曾被归类为军火贸易，我们当中一些人曾被当作军火贩子，然而一旦密码术

被内置于浏览器中并被银行业采用，这就形成了一股足够强大的游说力量来阻止对它的禁用——尽管我承认这些还只是酝酿中的步骤。

雅各布·阿佩尔鲍姆：这里的麻烦在于这种对隐私的担忧是错的。让我们老实说吧，认为在有互联网和在没有互联网的情况下，经济计算有所不同，这种假设是错误的。当我来到英国，我需要换一些英镑，我就必须上交我的社会保险号，这是我在美国的唯一身份证明，我还必须上报姓名，必须把身份跟一个银行账户关联起来，还必须给他们一笔钱。他们会记下所有这些序列号，他们会得到所有这些信息，然后他们会把这些全都报告给联邦政府。就是这么回事。实际上，在美国要取得外汇更加困难，因为我们跟其他地方都相距太远。然而，对货币的控制有这样一种历史趋势，它并不仅仅与互联网有关。事实上，据我所知，银行里的ATM记录着现金的序列号，追踪并分析现金的流动，查看这些现金的支出和持有人对它的使用。

如果我们考察一下这套系统，再联系一下互联网，就会发现，将活动转移到网上进行并不会改善我们的隐私——事实是，这些系统使隐私问题变得与最初一样糟糕。从这个意义上说，我觉得考察一下互联网之前的世界趋势是非常重要的，可以看出我们到底在走向何方。人们发现，如果你很有钱，你就可以为自己的隐私买一份优质保险；如果你没钱，你几乎肯定没有任何隐私可言。而互联网的情况甚至更糟。像比特币这样的东西是通往正确道路的一小步，因为只要它跟像Tor这样的匿名通信渠道相结合，Tor就允许你真正地向维基解密发送一个比特币，而任何监视到这笔交易的人只会看到一个Tor用户发送了一个比特币而你接受了它。这样做是可能的，在某种程度上这甚至比现金交易还好。

朱利安·阿桑奇：我们都在讨论通信隐私和发表权利的问题。这些都是相当容易理解的——这是由来已久的——另外，实际上，记者们也爱谈论它，毕竟这是在保护他们自己的利益。其实每当CIA观察一笔经济交易，他们能看到这是从某地的某人转移给某地的某人，然后他们就能对这笔交易的价值和重要性做到心中有数。所以，实际上，难道不是经济交易的自由或隐私比言论自由更重要吗，因为经济交易实际上是支撑整个社会的基础？

雅各布·阿佩尔鲍姆：它们似乎是内在相关的。我觉得你可以在这一点上看出美国密码朋克和欧洲密码朋克的区别，因为大多数美国密码朋克都会说它们绝对是同等重要的。因为人们认为在有自由市场的社会中，一个人会为自身的利益发声。

朱利安·阿桑奇：一个人会为自身的权力花钱。

雅各布·阿佩尔鲍姆：正是如此。我不是说这种观点是对的，这可以说是一种右派的主张，也许这不是我们想要的。也许，比如说，我们想要的是一种受到社会约束的资本主义。

朱利安·阿桑奇：让我们从一种更单纯的情报视角来看待这个问题：你得到了一笔1000万美元的情报预算。你可以监察人们的邮件往来，或者对人们的经济交易进行全面监控。你会选哪一种呢？

安迪·米勒–马贡：不错，现在他们会说："很好，我们只需要强迫这些支付公司和银行使用互联网，这样我们就可以两者兼得了。"而这就是他们实际所做的。所以，关键在于这里没有直接逃脱的办法。你可以做一些事情，像是使用Tor来保护你的通信、给你的电话加密、收发安全的短信，但涉及金钱，事情就复杂多了，我们有所谓的反洗钱法之类的法律条文，他们告诉我们说，贩毒团伙和恐怖主义组织在滥用这些基础设施做坏事。

雅各布·阿佩尔鲍姆：这就是信息末日启示录的骑士。

安迪·米勒–马贡：实际上，我对增加监控公司的透明度，以及政府在这些事情上的支出的透明度非常有兴趣。问题是当我们只为这种金钱系统提供全面匿名性时，我们会买什么？实际上会发生什么？我认为这会把事情带到有趣的领域，人们会更轻易地说："你知道，我可以提高音量，我可以走进议会，但我也可以收买某些政客。"

热雷米·齐默尔曼：你是在说美国，是吧？

雅各布·阿佩尔鲍姆：它并不是匿名的。

安迪·米勒–马贡：我不确定这仅限于美国。在德国，我们其实不管这叫腐败，我们管它叫"购买政客妻子画作的基金会"，所以这是艺术品交易或其他领域的事。我们给它取了更好听的名字：在法国，也许你们管它叫"联谊会"；在其他地方也能叫它"招妓"。

热雷米·齐默尔曼：这在美国最典型，因为政治体系与金钱的联系是如此密切。劳伦斯·莱斯格在持续关注版权问题十年之后，说他放弃了修正版权法的尝试（他并没有真的放弃），因为他发现，问题并不在

于政客们对什么是一项好的版权政策的认知，而在于这个行业中存在太多与政治有联系的参与者在推动这种糟糕的版权制度。[14]这才是症结所在。

朱利安·阿桑奇：热雷米，你确定这是个问题？也许事实上，这是一个好的标志，说明那些行业是有生产力的……

安迪·米勒–马贡：我觉得魔鬼的代言人在喝我的威士忌。

雅各布·阿佩尔鲍姆：看他能不能真的完成这场宣判，不要放弃。出招吧，钓鱼大师。

朱利安·阿桑奇：这些有生产力的行业为整个社会创造财富，它们拿出一部分钱来粉碎那些源于浮夸宣传的政治神话制造出来的随意立法，以确保它们可以继续保持生产力。而做这件事的最好方法，就是去买通国会议员，从这些富有生产性的行业中抽调人力去修改法律——以此来保持这个行业生产力的延续。

雅各布·阿佩尔鲍姆：等等——抓住你了。行吗？行吗？就现在，行吗？不行啊。

朱利安·阿桑奇：怎么了？

雅各布·阿佩尔鲍姆：有一堆原因，除了一点，那就是这里面的反馈链是极其负面的。举例来说，我相信加州最大的政治献金者之一是监狱保卫联合会，这里一部分原因在于他们愿意为更严酷的法律而游说，并不是因为他们关心法治，而是因为这能刺激就业。[15]于是，你看到这些人在游说建造更多的监狱，关押更多的人民，判处更长的刑期，他们积极从事这种活动的意义何在？他们的做法是不断利用行业劳工已经得到的好处去进一步巩固、扩张国家授予他们的垄断权。

朱利安·阿桑奇：所以他们只是利用这些利润去实现从真正有生产力的行业到没有生产力的部门的财富转移？

雅各布·阿佩尔鲍姆：你可以这样总结。

朱利安·阿桑奇：但也许这只是一小部分。每一个系统都可能被滥用，也许参与这种财富转移的搭便车者只是很小的一部分，而实际上大

多数游说以及对国会施加的影响确实来自富有生产力的工业界，这些行业要确保法律继续准许其保持生产力。

雅各布·阿佩尔鲍姆：但你可以很容易推算出来，因为你可以观察到是哪些人愿意促进寻租活动，愿意限制其他人打开局面的自由，在那种局面中这些人不会上升到他们今天所处的地位。当他们在做那些事情的时候，你就知道事情有问题，他们只是在保护自己的既得利益，他们本质上是在创造一种剥削——通常靠打感情牌，他们会说："老天啊，要阻止恐怖主义，阻止儿童色情，阻止洗钱，对毒品宣战。"也许这些事情在它们最初被提出来的场合中都是完全合情合理的，因为一般来说我们也都认为这些是坏事，因为其中的每一件都包含着危险成分。

安迪·米勒–马贡：我想回到版权问题，再给你另外一个例子——汽车刚出现时引起了广泛的争议。经营载客马车业务的公司害怕这将抢走它们的生意，事情的确如此，但也许它也是有意义的。我曾受邀给德国电影公司的联合会做演讲，在我讲话之前，一位来自柏林的大学教授非常有礼貌地谈到了人类的进化和文化的发展，说复制并加工思想是一个关键因素，就像电影的制作就是选择主题并对其进行戏剧化表达。在他谈了40分钟后，主持人粗暴地打断了他，然后说："好吧，在听了你刚刚说的那些之后，我们似乎应该把偷窃也合法化，让我们看看这位来自混沌俱乐部的伙计有什么要说的吧。"然后我就在想："喂，搞什么鬼？如果我把我想的都说出来，他们怕是不会让我活着离开这里吧？"所以，某些行业就是有这种无助于进化的商业案例。这就是自私，躺在他们的退化动机上，甚至把垄断弄得更严重。当盒式录音带出现时，他们也觉得唱片工业这下要完了。而事实正相反，唱片工业得到了迅猛发展。问题是，应该采取什么政策？我们可能以某种积极的方式来规范这些事情吗？

朱利安·阿桑奇：我只是好奇我们是不是真的不可能把美国的那些实践给标准化，把一切都规范化，这样只要单纯地收买参议员或者收买参议院的选票不就行了？

热雷米·齐默尔曼：不行，绝对不是。

安迪·米勒–马贡：假设我们有这笔钱。

朱利安·阿桑奇：对，让一切都公开化，在一群买家中进行拍卖。

安迪·米勒–马贡：但军工部门总是会有更多钱。

朱利安·阿桑奇：不，我认为不会。我真心认为军工复合体可能会相对边缘化，因为他们擅长的是在一个封闭体系中活动，躲在门背后进行暗箱操作，而在一般的市场竞标中，他们未必强过其他产业。

雅各布·阿佩尔鲍姆：在那种体系中存在着本质上的不平等。

热雷米·齐默尔曼：从一种经济自由的、反垄断的角度看，当你说让主导的参与者来决定政策的时候，我可以用最近十五年互联网的经验来回答你，创新是所谓的从下而上的，新的实践从无到有产生出来，一群人在车库中发明出的技术传遍了世界。

朱利安·阿桑奇：几乎所有发明都是如此，苹果、谷歌、YouTube都是如此。

热雷米·齐默尔曼：所有。互联网上发生的所有事都是在不为人知中发生的，几个月或几年之后却出现了爆发式的发展，所以你不可能预测出下一个创新是什么，创新的速度如此之快，远远超过政策制定的过程。

所以，当你设计一项对今日市场产生影响的政策时，它针对现在的各种公司和参与者之间的强关系，如果你加强了一项已经足够强的政策，你可能是在阻碍新的、更有效率的参与者的出现。

朱利安·阿桑奇：监管应该用来确保自由的市场。

热雷米·齐默尔曼：那是当然，你必须去对抗垄断，你需要拥有这种凌驾于公司权力之上的权力去惩罚坏的行为——但是我在这里的观点是政策必须适应社会，而不是相反。版权战争让我们有这样的印象，即立法者努力想要全社会都做出改变，以适应一种由好莱坞定义的框架，他们说：“你们的新文化运动是不道德的，所以，如果你们不想自行了断，那我们就来设置法律工具来阻止你们去做你们自以为是的好事。”这不是制定好政策的方式。一项好的政策是观察世界并且适应世界，以纠正错事、促成好事。我相信，如果授权给最有权势的行业参与者去决定政策，就绝不会得到这种政策。

安迪·米勒–马贡：我刚刚一直在试图让我们思考一个好政策是什么

样的。在我看来，你刚才的那种总结，就目前阶段来说，有点儿过于复杂了，我试着把它简化一下。有一个叫海因茨·冯·福尔斯特（Heinz von Foerster）的家伙——控制论的教父——曾经制定出一套规则，其中之一是“总是以某种增加选择的方式来行动”。[16] 所以通过政策、技术，或者其他东西，你总是能得到更多而不是更少的选择。

朱利安·阿桑奇：就像象棋策略。

安迪·米勒–马贡：有人提出给予金钱交易更多的隐私可能会造成负面效果，所以我们需要想一想：“现在的金钱系统有一个特定的逻辑，问题在于我们如何防止金钱系统接管其他领域？”因为金钱系统有这种能力——不像通信部门——可以影响和全面限制人们在其他领域的选择。假如你可以雇用职业杀手去做某件事，或者假如你购买武器并与其他国家一起卷入一场战争，你就是在限制其他人生存的选择、行动的选择。如果我把更多的钱投入到通信中，那么更多人就获得更多的选择。如果我把更多的武器投入市场……

雅各布·阿佩尔鲍姆：不对，你越是有能力进行监控，你就越有控制权。

安迪·米勒–马贡：这是限制包括通信监控技术在内的武器贸易的另一个好论据。

雅各布·阿佩尔鲍姆：当然，你想限制我出售武器的能力，你怎么能够做到呢？你怎么限制我转移财富的能力？——还是要依靠通信网络。这是美国的援助中最令人反感的事情之一——有一大堆理由让人们对此感到反感——他们显示出，财富就好像是计算机系统中的一系列比特。通过各种有效的方式，某些人试图获得更多高位比特，那么问题出在哪儿？如果你可以欺骗这个系统，把你的比特设定到高位，那这个系统的价值何在？而且其他努力求生的人首先都不被告知是否还有值得翻转的比特。[17]

安迪·米勒–马贡：所以，你的意思是我们需要一个完全不同的经济体系？因为今天的价值并不依附于经济价值？

雅各布·阿佩尔鲍姆：不是，我的意思是存在一种经济价值。

安迪·米勒–马贡：你可以干坏事，通过干坏事来赚钱，你也可能做

了好事而一分钱也拿不到。

雅各布·阿佩尔鲍姆：不是，我说的是你不能切断经济与通信之间的联系。我不是在讨论我们是否需要一个不同的经济系统。我不是经济学家，我只是想说在通信系统中存在某些价值，这些价值存在于通信的自由之中，就像存在于实际交易的自由中一样——我们有权给你某些东西以换取你的劳动，就像我有权解释一个观念，而你有权告诉我你对它的想法。我们不能说经济体系存在于某种真空中。通信系统是直接与这种经济体系相结合的，这是生活的一部分。

如果我们想得到一个对于朱利安提到的三种自由的还原论的概念，那么这就明显与行动的自由密切相关——不使用可追踪的货币，你现在甚至都买不到一张机票，不然你就要被标记了。如果你走进机场，想要在当天用现金买一张机票，你就被标记了。

你会遭到额外的安检搜身，没有身份确认你就不可能起飞，而且如果你真这么倒霉，用信用卡买了你的机票，他们就会记录你的一切事情——从你的IP地址到浏览器。我有通过《信息自由法案》得到的数据，那是移民和海关执法局多年来关于我的记录，因为我认为有朝一日看看其中的差别可能很有意思。果然，记录中有罗杰·丁格勒戴，他曾帮我买过一张公务机票，用的是他的信用卡，他买机票时的住址，他当时使用的浏览器，一切与那张机票有关的事情都被结合在了一起。

朱利安·阿桑奇：而且这些记录都会进入美国政府，而不会只保存在商家那里，是吧？

雅各布·阿佩尔鲍姆：对。商业数据被搜集起来，报送给政府，他们是勾结在一起的。我发现真正疯狂的是，这本质上是你谈到的那三种自由的结合。自由旅行是我的权利，我能购买那张机票或让其他某个人买那张机票，我也能够有效地发表演讲——但如果我要旅行到某个地方去做一个演讲，我就必须要在两个领域中做出妥协。而且，实际上这影响到我去演讲的能力，特别是之后我发现他们搜集了数据，并把数据结合在了一起。

注释

1 ．对于这个问题，维基解密所发布的美国外交电报中有大量精彩的内容。更多有趣的讨论可以参考以下电报（根据电报参考号排列，所

有链接均访问于2012年10月24日）：07BEIRUT1301：http://wikileaks.org/cable/2007/08/07BEIRUT1301.html；08BEIRUT490：http://wikileaks.org/cable/2008/04/08BEIRUT490.html；08BEIRUT505：http://wikileaks.org/cable/2008/ 04/ 08BEIRUT505.html；08BEIRUT523：http://wikileaks.org/cable/2008/04/08BEIRUT523.html。

2 . 参见10MOSCOW228号电报，载于维基解密，http://wikileaks.org/cable/2010/02/10MOSCOW228.html（访问于2012年10月24日）。

3．更多关于对美国公民安瓦尔·奥拉基（Anwar al-Awlaki）及其子阿卜杜勒拉赫曼·奥拉基（Abdulrahman al-Awlaki）的合乎程序的谋杀，参见格伦·格林沃尔德（Glenn Greenwald）的报道“The due-process-free assassination of U. S. citizens is now reality”，载于《沙龙》，2011年9月30日，http://www.salon.com/2011/09/30/awlaki_6；以及“The killing of Awlaki 16-year-old son”，载于《沙龙》，2011年10月20日，http://www.salon.com/2011/10/20/the_killing_of_awlakis_16_year_old_son。在想象不出还有什么行为比发展一个完全不可问责的秘密执行机构更能粗暴地践踏共和国的基本蓝图，而且，这个秘密执行机构同时还在搜集所有公民的信息，并使用一种‘部署矩阵’（disposition matrix）来决定执行哪些惩罚。经典的反乌托邦政治已经走向了现实。”——格伦·格林沃尔德，“Obama moves to make the War on Terror permanent”，载于《卫报》，2012年10月24日，http://www.guardian.co.uk/commentisfree/2012/oct/24/obama-terrorism-kill-list。（所有链接均访问于2012年10月24日）

4．更多信息请参考“匿名书单”（The Anonymity Biblio-graphy），关于匿名的论文精选，由罗杰·丁格勒戴和尼克·马修森（Nick Mathewson）管理：http://freehaven.net/anonbib（访问于2012年10月24日），乔姆币（Chaumian）是中央处理的，但使用了密码术来确保交易的匿名。与乔姆币相反，比特币（本文讨论的另一种电子货币）的所有交易都是公开的，但并不存在一个中央的货币权威。

5．更多有关对维基解密金融封锁的信息，参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

6 . 朱利安这里提到的是英国增加电子追踪器使用的计划。“Over 100,000 offenders to be electronically tagged”，载于《卫报》，2012年3月

25日，http://www.guardian.co.uk/society/ 2012/mar/25/prisons-and-probation-criminal-justice（访问于2012年10月22日）。在这场讨论发生之时，朱利安正处于软禁之中，等待着他的引渡案的结果。2010年12月，朱利安未经起诉便遭到单独囚禁，在支付了超过30万英镑的保释金后，朱利安的拘留转为软禁。作为保释的条件之一，他被限制在特定时段内只能待在一个特定的地方，脚踝上被强制佩戴电子追踪器，该追踪器由一家与英国政府签约的私人安保公司操作。朱利安的行动被控制到了这种程度，他被迫每天在特定时刻去警局报到，这种状况持续超过了550天。就在本书出版之时，朱利安被禁闭于位于伦敦的厄瓜多尔大使馆内，并被伦敦市警方持续包围。2012年6月，朱利安进入大使馆寻求政治避难，以躲避美国政府及其盟友的迫害。他在2012年8月获得避难权。

7．“Is CCA Trying to Take Over the World?”，载于美国公民自由联盟，2012年2月21日，http://www.aclu.org/blog/prisoners- rights/cca-trying-take-over-world；“Passing House Bill will worsen already pressing civil rights issue”，载于ANNARBOR.com，2012年8月2日，http://annarbor.com/news/opinion/passing-house-bill-will-worsen-already-pressing-civil-rights-issue；参见“Goldman Sachs to invest $9.6m in New York inmate rehabilitation”，载于《卫报》，2012年8月2日，http: //www.guardian.co.uk/society/2012/aug/02/goldman-sachs- invest-new-york-jail（所有链接均访问于2012年10月24日）。

8．比特币（http://bitcoin.org）是经典密码朋克理念第一次真正成功的诠释：一种加密的数字货币。比特币将在本书中得到详细讨论，但是关于比特币技术及其背后哲学的精彩介绍和解读可以参见，“Understanding Bitcoin”，载于半岛电视台网站，2012年6月9日，http://www.aljazeera.com/indepth/opinion/2012/05/20125309437931677.html访问于2012年10月22日）。

19．电子黄金是1996年出现的一种数字货币和商业。电子黄金的拥有者和经营者被美国司法部以“参与阴谋洗钱”的罪名起诉。他们承认有罪并被判处缓刑、在家服刑和社区服务。判刑的法官称他们并未打算从事非法活动，因而应当得到宽大处理。参见“Bullion and Bandits:The Improbable Rise and Fall of E-Gold”，载于《连线》，2009年6月9日，http://www.wired.com/threatlevel/2009/06/e-gold（访问于2012年10月22日）。

10．在因特网之前，X.25网是与电话网平行存在的用于数据交换的主要全球网络。X.25网的计费基于发送和接收的数据量，而非电话网的连接长度。被称为PAD的网关允许使用调制解调器或声音耦合器从电话网接入X.25网。更多细节参见维基百科：http://en.wikipedia.org/wiki/X.25（访问于2012年10月24日）。

11．大卫·乔姆是密码学家和加密通信协议的创制者。他是数字货币技术的先驱，他引入了电子现金（eCash），这是最早的匿名加密电子货币之一。

12．对于此事的负面新闻报道参见“Bitcoin implodes,falls more than 90 percent from June peak”，载于arstechnica，2011年10月8日，http://arstechnica.com/tech-policy/2011/10/bitcoin- implodes-down-more-than-90-percent-from-june-peak（访问于2012年10月22日）。

13．一个事例，参见“The Underground Website Where You Can Buy Any Drug Imaginable”，载于Gawker，2011年6月1日，http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable（访问于2012年10月22日）。

14．劳伦斯·莱斯格早期的工作关注版权和文化［例如2004年出版的《自由文化》（*Free Culture*）］，近年来他的兴趣转移到国会游说活动对美国民主的腐蚀上。参见莱斯格的wiki：http://wiki.lessig.org。

15．加州惩治警官协会（The California Correctional Peace Officers Association）是加州一个具有影响力的特殊利益集团，它在加州选举中常规的捐款数额达到7位数，尽管以年度来算，它并不是最大的单笔竞选捐助者。参见“California reelin”，载于《经济学人》，2011年3月17日，http://www.economist.com/node/18359882；以及“The Golden State’ Iron Bars”，载于Reason，2011年6月，http://reason.com/archives/2011/06/23/the-golden-states-iron-bars。亦可参见金钱与国家政治全国研究所（the National Institute for Money in State Politics）的网站FollowTheMoney上关于加州惩治警官协会的条目：http://www.followthemoney.org/database/topcontributor.phtml?u=3286&y=0。（所有链接均访问于2012年10月22日）

16．海因茨·冯·福尔斯特（Heinz von Foerster，1911—2002）是一位美籍奥地利裔科学家，也是控制论的奠基人之一。他所谓的“道德命

令”（ethical imperative）或通用格言是“行动总是以某种方式增加选择”，德语原文为“Handle stets so, daß die Anzahl der Wahlmöglichkeiten größer wird”。

17 . 雅各布把这个洞察归功于约翰·吉尔莫。

[1] 纳斯鲁拉被美国和以色列视为恐怖分子头目，曾遭遇“斩首”行动，而阿桑奇被美国政府视为高科技恐怖分子，希拉里在国务院内部会议上曾提议对其实施无人机暗杀。雅各布这里的意思是提醒阿桑奇注意身份，当心被暗杀。——译者注

审查

朱利安·阿桑奇：雅克，谈一下你在美国机场被扣留的经过吧，为什么要扣留你？

雅各布·阿佩尔鲍姆：他们声称“你知道这是为什么”。

朱利安·阿桑奇：但是他们自己不说？

安迪·米勒–马贡：我能来总结一下吗？因为技术安全和政府事务的安全完全是可以分开来看的两件事。你可以搞一个在技术上完全安全的系统，而政府会想，这可不好，因为他们所认为的安全就是他们能够窥探、能够控制、能够破解技术上的安全。这跟雅克要登上飞机去杀人或者去劫机什么的无关，而是因为雅克有能力通过旅行到达其他国家、对人们发表演讲、传播观点来影响政府事务。这才是这个时代对政府来说最危险的事——对于政策，人们有比政府更好的见解。

雅各布·阿佩尔鲍姆：非常感谢你这么恭维我，但我其实只想指出事情比这还糟糕，因为他们能够搜集所有人的数据。这些都发生在我真的去做了某些有意思的事情之前，当时的事实仅仅是我在旅行，而这个系统、这个体制推动了信息的搜集，在我还没被阻止去做任何事之前它就发生了，在我被赶出黎巴嫩之前，在美国政府特别针对我之前，它就发生了。

安迪·米勒–马贡：可能他们能够预测，可能他们在你行动之前就发现你了。

雅各布·阿佩尔鲍姆：他们当然能，部分是因为数据搜集。但是他们总是给我不同的回答。他们常用的一个回复，一个通用回复，是“因为我们能”。那我就说了：“好的，我不是在质疑你的权威——好吧，我确实质疑你的权威，但不是现在——我只是想知道这事现在怎么会发生在我身上。”人们总是对我说，“这不是显而易见的吗？你为Tor工作”，或者，“你坐在朱利安旁边，你还能指望什么？”让我感到惊奇的是，这些不同的人，通常是美国海关和边境保护局以及美国移民和海关执法局

的人，他们每个人都告诉我，是因为他们有权力这么做，而不是别的什么原因。有时他们还对我胡扯什么“记得‘9·11’吗？这就是原因”或者“因为我们想让你回答一些问题，在这里你可没多少权利，或者至少我们不承认你的权利”。

在这种情形下，他们不让你接触律师，也不给你提供厕所，但他们会提供水，会给你喝点儿什么，像一杯利尿剂之类的，以便让你相信你确实需要在某种程度上配合他们。他们就是这样对你施压的，出于政治原因。他们会问我一些问题，问我对伊拉克战争作何看法，对阿富汗战争有何感想。基本上他们的每一个步骤都是在重复FBI在“反谍计划”（COINTELPRO，1956—1971年在美国国内实施的大规模秘密调查项目）中所采取的战术。比如，他们试图特别强调他们有权力改变我个人的政治生活，他们试图逼迫我，不仅要改变我的政治生活，还让我向他们坦白自己头脑中在想些什么。他们还没收了我的财产。我也不能具体地谈论这些发生在我身上的事情，因为这处在一个阴暗的灰色地带，我并不确定我是否被允许谈论这些。我确实知道其他一些人也遭遇过这样的事，但我从没听他们说起过。

有一次我在多伦多皮尔逊国际机场，刚参加完一个活动，正要回家探亲，飞回西雅图——我当时住的地方——然后他们就扣留了我，他们将我带去做二次检查，然后是三次检查，最后是进拘留室。他们把我扣留得太久，以致当我终于被释放时已经错过了航班。诡异的是，因为羁押我的地点严格说来是在加拿大国境内的美国领土，所以根据一个规定，如果你错过了航班而距离下一个航班时间又很长，那你就必须离开这里。由于被扣留得太久，我就被踢出美国领土了，不得不进入加拿大，然后租一辆车再穿越边界。我到边境时，他们又问，“你在加拿大待了多久？”我回答，“五个小时加上在多伦多的扣留”，所以我大概在加拿大待了八个小时，然后他们说：“那好吧，进来，我们要再次扣留你。”然后他们拆了我的车，拆了我的电脑，把所有东西翻了个遍，还扣留了我。他们给我半个小时的时间去上厕所，你可以说他们也算大发慈悲了。这就是所谓的边境搜查特权——因为他们声称他们有权这么做，而没人能挑战他们的权威。[1]

朱利安·阿桑奇：所以，这就是你的遭遇，但是我跟一些中国人谈过，当他们谈到防火墙——用我们西方人的话来说就是审查，他们的关注点其实并不是审查。他们关注的是，为了实现互联网审查，你必须要同时实现互联网监控。事实上，这对我们也是一样。一旦人们意识到了

这点，这会改变他们的行为，让他们在抗议各种权威的时候变得不那么坚决了。

雅各布·阿佩尔鲍姆：但那是对这种压力的错误回应。例如，他们在边境对我的骚扰并不是个例，自从“9·11”之后，甚至在那之前，每一个阿拉伯裔美国人都不得不遭遇这样的事。我只是拒绝让白皮肤和美国护照给我带来的特权被浪费在这里，我拒绝保持沉默，因为他们的所作所为是错的，因为他们在滥用职权。我们必须站出来反对这样的事，也有很多勇敢的人站出来以同样的方式反对这种审查制度，并为此做出过有效的工作。因为正确的回应不能是仅仅因为政府宣称他们有权这么做，我们就在屈服于这种压力。

热雷米·齐默尔曼：现在我们又谈到了政治，因为你说的基本上就是人们应该站起来捍卫他们的权利——但是人们也应该认识到为什么要捍卫自己的权利，并且有能力通过交流来捍卫自己的权利。我曾经有机会跟一些来自中国的人交谈——我不知道他们是否在政府中就职——但当我跟他们说到互联网审查时，我常常得到这样的回答：“这其实是为人民好。如果没有审查，就可能出现极端行为，出现我们所有人都不愿意看到的状况，所以政府需要采取这种措施来确保一切稳定。”如果你考察下中国的审查是如何运作的，你会发现，从技术角度来看，这算是世界上存在过的最先进的审查系统之一了。

雅各布·阿佩尔鲍姆：绝对是。

热雷米·齐默尔曼：我还听说在微博上，就是中国版的Twitter，政府有能力对某些标签进行筛选，以确保它们只能留在某个特定的省份。

雅各布·阿佩尔鲍姆：需要记住的关键一点是，当西方人谈论亚洲地区那些审查时，他们喜欢用到“其他人”这个词——就好像这只会影响到“其他地方”。重要的是认识到当你在美国使用Google搜索时，他们也会说出于法律要求，部分搜索结果被省略。当然，在审查的实施方式，以及对于如何审查、为何要审查和在何处审查的社会现实上，这两个地区的审查存在着差别，其中一个最大的区别其实就是体系结构。例如，在美国互联网的结构是相对去中心化的，在这方面它就很难实现中国式的审查。

朱利安·阿桑奇：西方审查的一大部分在于Google，而政府也可以审查Google。一大批援引了维基解密的网页都被Google的审查给过滤掉

了。

雅各布·阿佩尔鲍姆：对的，毫无疑问。而且正因为索引本身是自由的，你可以去做一个差异分析。

朱利安·阿桑奇：理论上是可以的。

雅各布·阿佩尔鲍姆：是理论上，而实际上现在世界各地也有些人从不同视角来考察这种差异，对审查制度的类型做检测研究。我认为重要的是要记住，审查和监控不仅是“其他地方”的问题——西方人总是喜欢说“伊朗人和朝鲜人如何如何需要匿名和自由，但在我们这里就不需要”。所谓的“在我们这里”，通常指的是“在美国”。但事实上这个问题并不只存在于那些压迫性的政治体制中，因为只要你处在政权的最高阶层，你就不会感受到压迫。我们认为英国是个很棒的地方，人们通常以为瑞典这地方也相当不错，但是你能看到，一旦得罪了当权者，你的下场也不会太妙。但是，朱利安总算还活着，对吧？所以显然，这就是自由国家的标志，这没错吧？

朱利安·阿桑奇：我是在艰难维持我目前的状态。但也许我们该谈谈西方世界的互联网审查了，这也相当有趣。假如我们回到1953年，看看当时的《苏联大百科全书》——当时这书到处在发行，这套百科全书有时会根据苏联的政治变动做一些修订。1953年，苏联秘密警察的首脑、内务部长贝利亚被撤职并受到处决，于是关于他的那部分，那些正面表述他的条目，就被编纂百科全书的机构给删除了，然后他们在所有百科全书中的这些部分打上修订补丁。我提到这个例子是因为它太露骨、太容易被发现了，这让这种企图都成了历史的一部分。然而，在英国，我们也看到《卫报》和其他主流报刊在偷偷地从他们的互联网档案库中删掉某些文档，而对此不作任何说明。你现在再去访问这些网页，试着去查找这些文档，比如去找找关于亿万富翁纳达米·奥奇（Nadhmi Auchi）欺诈案的故事，然后你会看到“页面未找到”，而且它们也从索引中被移除了。

让我来告诉你我跟纳达米·奥奇这件事的牵连。1990年伊拉克入侵科威特，导致了第一次海湾战争。科威特政府在流亡期间及回国的过程中都需要现金，于是它开始变卖各种资产，包括在科威特境外的炼油厂。纳达米·奥奇是一个英国商人，他在20世纪80年代初从伊拉克移民到英国，在伊拉克的时候他是萨达姆政权中的一位要员，当时他是科威特这些交易的经办人，之后他被指控参与1.18亿美元的非法佣金交易。

这是战后欧洲最大规模的腐败案调查。2003年，奥奇被判在Elf Aquitaine丑闻中犯有欺诈罪。然而现在呢，他还是通过他在卢森堡控制的集团注册了超过200家公司，另外通过巴拿马也注册了一部分。他还参与了战后伊拉克的通信建设承包工程和遍布世界的其他许多生意。[2]

在美国，奥巴马参议院竞选团队的筹款人托尼·雷兹科（Tony Rezko）是奥奇的长期合作伙伴，奥奇是他的金融顾问。类似的，奥奇和雷兹科跟伊利诺伊州前州长罗德·布拉戈耶维奇（Rod Blagojevich）也有瓜葛。雷兹科和布拉戈耶维奇都被判犯有腐败罪，前者于2008年，后者于2011年（在FBI通过电话拦截记录下布拉戈耶维奇试图出售奥巴马留下的参议员席位之后）。2007—2008年，奥巴马正在竞逐民主党总统候选人的时候，美国媒体开始调查奥巴马的关系网。他们查到了雷兹科，还报道了一些跟奥巴马的房屋交易有关的联系。2008年，就在审判前不久，雷兹科还从奥奇那里接受了一笔350万美元的转账，而且没有向法庭报告，他就是因此被判入狱的。于是美国媒体的调查转向了奥奇，就在那时，针对2003年的Elf Aquitaine丑闻及其在法国被定罪的大量报道，他授意他的英国律师事务所卡特–拉克（Carter-Ruck）发动了一场攻击，效果相当成功。他攻击英国媒体，甚至美国的博客，让我们所知的大量文章都被移除了。这些文章中的大部分，包括存档在英国报刊中的，就这样完全消失了，就好像它们从来没有存在过。这里也没有“我们收到了法律投诉，决定移除这些报道”的说明，连它们的索引都消失了。维基解密挖掘出了这些报道并重新发布了它们。[3]

雅各布·阿佩尔鲍姆：他们在擦除历史。

朱利安·阿桑奇：历史不仅被篡改，而且不再存在了。正如奥威尔的名言：“谁控制了现在，谁就控制了历史；谁控制了历史，谁就控制了将来。”在西方，这种对历史的擦除是难以发现的，而且这还仅仅是出版后审查。出版前的自我审查远甚于此，但是通常更难被发现。我们在维基解密跟全世界不同的媒体合作伙伴共同曝光邮件门的过程中发现了这件事，我们可以看出哪些媒体对我们的材料进行了审查。[4]

举例来说，《纽约时报》就对一封电报进行了编改，那封电报说通过在利比亚经营的石油公司发放了数百万美元，用以暗中对利比亚的相关人士施加政治影响。邮件中没有点名具体的石油公司——而《纽约时报》却对“石油服务公司”这个词做了编改。[5]–最明目张胆的编改恐怕是《纽约时报》对一封62页的电报的使用，这封电报关于朝鲜的导弹计

划、朝鲜是否向伊朗出售了导弹。《纽约时报》在一篇报道中使用了这封电报中的两段话，用来说明伊朗拥有能够攻击欧洲的导弹，而电报中剩余的部分却正好是反对这种观点的。[6]

《卫报》编改了一封有关乌克兰前总理尤利娅·季莫申科的电报，其中提到她可能隐瞒了她在伦敦的财富。[7]《卫报》过滤掉了对哈萨克斯坦权贵普遍腐败的指控——这里甚至没有一个人被点名——以及对在哈萨克斯坦经营业务的意大利能源公司ENI和英国天然气公司的腐败指控。[8]基本上，只要某个有钱人在电报中受到了指控，《卫报》都会将其过滤掉，除非《卫报》在制度议程上反对那个有钱人。[9]所以，举个例子，在一封关于保加利亚有组织犯罪的电报中出现了一个俄罗斯人，《卫报》就把这封电报弄成像是整个事情都关于那个俄罗斯人，但其实那家伙只是这一长串跟保加利亚有组织犯罪有关的机构和个人名单中的一个而已。[10]《明镜》周刊也过滤掉了一段关于默克尔所作所为的内容——当然不是出于人权关怀，而纯属是对默克尔的政治考量。[11]这样的例子太多了。[12]

安迪·米勒–马贡：如果你看一看我们的地球，你会发现，我们所理解的信息自由以及信息流动的自由，在某种意义上说，是一个非常激进的新概念。我不认为这在欧洲和其他国家之间存在多大的不同。的确，某些国家是有民主架构，这表明你可以阅读和理解，甚至也许还能合法地对抗审查制度，但这并不意味着审查制度在这里不存在，尽管在有些国家抗衡会更艰难。

朱利安·阿桑奇：就我在西方的经验来看，这里的审查制度要复杂精妙得多，它通过多个层面的间接途径来混淆正在发生的事实，这些层面可以用来否认正在发生的审查。你可以把审查制度想象成一座金字塔。只有金字塔的塔尖故意露出了沙面。这个塔尖就是公共诽谤诉讼、谋杀记者、被军队抢走相机，诸如此类——所谓公开承认的审查。但这只是整个审查制度中最小的一部分。在塔尖之下，接下来的一层就是那些不愿意被暴露在塔尖的人，这些人进行自我审查，以免被推向塔尖。再下一层就是各种形式的经济诱导，或者赞助诱导，让人们去报道某件事情。再下一层就是原始经济——只去写那些划算、有赚头的故事，甚至都不必考虑上层的经济因素。然后，再下一层就是读者的偏见，这些人只受过片面的教育，所以，一方面，他们很容易受到假消息的操纵；另一方面，你又不能告诉他们复杂但真实的信息。最后一层就是信息的传播——例如，有些人没法接触到某种语言的信息。所以这就是审查金

字塔。《卫报》在邮件门中所做的编改处于这个金字塔的第二层。

目前，这类审查是不被承认的，因为它们发生在暗处，也因为并不存在对某个特定主张进行审查的指示。记者很少得到指示，说“不要报道任何有关那个的东西”，或“不要发布这个事实”。相反，是记者认识到他们被期望如何做，因为他们了解他们希望取悦或巴结的那些人的利益所在。如果你表现得好，他们就会拍拍你的脑袋，给你赏赐；如果表现不好，那你就什么也得不到，就这么简单。我总是喜欢打这个比方：存在于苏联的审查制度，那种被西方大肆宣传的审查制度——半夜踢开记者家的门把他们带走——现在被倒转过来了。现在，我们在等着有这么一天，把真相从记者那里“带回来”，因为它们脱离了庇护，不再履行它们的职责。记者们放弃了职责，真相也就被带走了。西方社会很擅长对审查进行洗白，并将权力的运作制度化，因此，在这个高度财政化的社会中，任何通过这种审查还能留存下来的公开言论都很难动摇真正的权力关系。

安迪·米勒–马贡：热雷米提到过小纳粹。

雅各布·阿佩尔鲍姆：我们又回到小纳粹的问题了。

热雷米·齐默尔曼：问题合二为一了。

安迪·米勒–马贡：小纳粹的问题很好地总结了德国，或许是欧洲审查争议的一部分。由于历史问题，德国自然见不得任何仇恨言论——像是在互联网上的那些内容，如果你告诉人们，对互联网进行限制是为了打击恋童癖，那你就想怎么限制都可以了。同样，一篇关于数据存储的欧盟委员会工作论文争辩道：“我们应该多谈谈儿童色情问题，那样人们就会支持我们了。”[13]

朱利安·阿桑奇：我们能就这个问题多谈一点儿吗？如果我们只针对某项事物进行审查，比如说儿童色情，那么为了从人们浏览的东西中过滤出儿童色情的内容，我们就需要监视每个人在做什么。我们需要建立那样的基础设施。就为了审查单单一项内容，我们就得建立一个大规模的监听和审查系统。

安迪·米勒–马贡：这些可以从这套机制的细节中看出——在德国，无论你要发表什么内容，所谓的事前审查系统都要求你为此指定一位法律负责人。所以，大致说来，如果你要发表什么东西，无论是发表在一

篇论文中，还是发布在互联网上，只要你没有说明谁对这些内容承担法律责任，那你就已经违法了。这就是说你被摊派了这种责任，比如某人因为散布儿童色情或者仇恨言论而触犯了法律，那你就可以说：“那好，看看这家伙住在哪儿，我们去抓住他，然后把这些东西从网上删掉。”

朱利安·阿桑奇：那就是说，我们以审查发布者代替了审查读者。

安迪·米勒–马贡：对，而且这是在监视特定内容。我认为并不是所有东西都一直需要得到公开，关于仇恨言论的问题，这里可能涉及某些人的私人住址之类的东西，在这种情况下我是不会赞同的。

朱利安·阿桑奇：但是，安迪，这是典型的德国作风。为了做某件事，为了判定哪些东西可以接受、哪些东西不可接受，你不得不组建一个委员会，就得为这个委员会选派代表，还得为这个委员会搞一套选派代表的程序……

安迪·米勒–马贡：对，我们需要所有这些垃圾。德国人在“二战”中的杀戮——纳粹所做的每一件事，每一项他们掠夺的财产，他们都会给你个收据，还列出了清单。完全的官僚做派。你可以说德国人无理杀害了很多人——这是真的——但是他们是在按官僚程序办事。这就是德国。

朱利安·阿桑奇：如果你要让某人来裁定哪些东西应该被审查、哪些东西不该被审查，那你就必须做两件事。首先，你需要建立一套技术体制去实施这样的审查，你必须建立一个全国范围的审查机制来有效地执行审查。其次，你需要组建一个本质上是秘密的委员会，因为除非是秘密的，不然它就根本没用，于是你又需要秘密司法..

安迪·米勒–马贡：你知道吗？我们在德国就有这么个好原则。

雅各布·阿佩尔鲍姆：就一个？

安迪·米勒–马贡：这个原则就是，如果一项法律的适用是不切实际的，那这项法律就不应该存在。如果一项法律没有意义，比如说禁止风力磨坊或其他什么，那我们就会说，“嘿，来吧，忘掉它”。如今我们都受到互联网的鼓舞，我们随着互联网的成长而了解它，我们受到信息自由流动的鼓舞，意识到自由就是不受限制、不受封锁、不受审查、不受

过滤。于是我们将对信息自由流动的理解运用到整个地球的事务上，而且它也已经大致被运用到了整个星球的事务上了。当然，我们看到，政府受到信息自由流动的影响，它是如何对此施加权力，以及审查制度是如何运作的，可以是事前审查、事后审查或无论什么审查。从发生的这些复杂的冲突中，我们可以学到所有这些事。问题在于，我们怎么看政府或者怎么看“后政府组织”（Post-Governmental Organisation）的未来——也许维基解密就是第一个，或第一代后政府组织中的一个，因为我可不确定政府就是应对我们星球上所有问题的正确答案，比如说环境问题。

朱利安·阿桑奇：甚至政府本身也是不确定的，什么是政府、什么不是政府，这之间的界限很不明确。这种界限现在变模糊了。政府占据着物理空间，但维基解密占据了互联网空间。互联网空间是嵌入现实空间的，但是被嵌入的对象与嵌入体之间的关系很复杂，对嵌入体来说，并不容易分辨出被嵌入的对象是否成了它的一部分。所以，这就是为什么我们有一种赛博空间的感觉——它其实是存在于某处的一些其他领域——这来自它的非直观性、复杂性和普遍性。你在某个地方阅读互联网上的某篇文档和你在其他地方阅读这篇文档，或在未来阅读这篇文档，这之间并没有差别——这就是它的普遍性。所以，在这种程度上说，由于一个占据了赛博空间的组织擅长将它的信息散布于底层的嵌入体，或许正是因为这种地理限制，我们成了一个后国家组织（post-state organisation）。

我不会把这个类比发挥得太远，毕竟我自己就被软禁着。无论人们是否意识到，国家的强制暴力明显对我们所有人起作用。但是其他的媒体似乎将我们视为一个无国籍的媒体组织，他们对这种无国籍性质的重要性的认识也是非常正确的。我总是习惯说：“你以为新闻集团是什么？它就是一个大型跨国组织。”尽管如此，新闻集团的这种组织结构是它的关键，这就是为什么它在英国有电话窃听丑闻的大麻烦，在美国它又一直在巴结体制权贵。但是，如果一个组织的资产首先在于它的信息，那么由于运用了密码术，就很难阻止它以某种形式进行跨国传播。这也是为什么我们遭到金融封锁——我们组织的其他方面更难被压制。[14]

雅各布·阿佩尔鲍姆：如果我们用乌托邦的术语来讨论这个问题，我们就必须回顾得稍微远一点儿。你问到关于我受到的骚扰，你问到西方的审查制度，还有我之前提到的奥巴马的定点清除计划，他们说这是合法的，因为这里有合法的程序，因此这被归结为一个法律程序问题。

朱利安·阿桑奇：对，一个秘密程序。

雅各布·阿佩尔鲍姆：我们也可以把这个问题联系到约翰·吉尔莫。约翰·吉尔莫有一个诉讼，关于他能否在美国匿名旅行，法院明确表示：“我们将援引一条秘密法。我们将依据这条秘密法，判定你是否被允许做这件事。”然后，在阅读这条秘密法时，他们发现事实上他被允许这么做，因为这条秘密法并没有限制他。他永远不会知道这条秘密法到底是什么。之后，作为对他胜诉的回应，美国运输安全管理局和国土安全部修改了政策，因为这表明这条秘密法在这种意义上是不具备约束力的。[15]

朱利安·阿桑奇：所以他们把它修改得更有约束力？

雅各布·阿佩尔鲍姆：通过官僚立法程序进行了有效的修改。但重要的是要注意到定点暗杀计划、人们在边境遭遇的骚扰、互联网审查制度，无论是听命于政府的审查还是听命于企业的审查，所有这些事情都联系在一起。而且，问题归根结底在于，在每一个我们看到出现这些问题的地方，政府都握有太多的权力。权力集中在这些领域而且吸引着滥用权力和贪图权力的人。而且，即使某些情况是合理的，我们也看得出，如果没有这种集中化、没有这种通向威权主义的趋势，世界可能会更好。

在这方面，西方也不例外，因为这表明如果你有一个网络安全的沙皇，这与另一个国家五十年前的国内安保部队的沙皇并没有多大不同。我们正在建立一种同样的威权控制结构，它吸引人们去滥用它，而我们却企图假装这种事情在西方会有所不同。在西方这也没有任何不同，因为存在着一个统治的连续体，从威权主义到个人意志主义。我不是在美国政治派别的意义上说这件事，而是在这种意义上说的：在这个统治连续体中，美国在很多很多方面都距离苏联非常远，但比起克里斯钦尼亚（Christiania）[16]这个位于丹麦哥本哈根中心的自治社区，它距离苏联就要近得多了。而我认为美国距离一个可能的乌托邦甚至更远。如果我们能去火星创建殖民地的话，我们可能会愿意移民去我们在火星上建立的世界，离极权主义和威权主义越远越好。如果我们没有那种乌托邦，就总是有所欠缺的。

热雷米·齐默尔曼：又来了，所有话题又被绑到了一起。当我们谈论集权，我们就谈到了体制。而当我们谈论审查制度，这又与集权有关，谁有权判定哪些内容人们可以接触、哪些不行，政府审查或者私人

进行的审查是否是滥用权力？我们有这样的例子：我们的网站laquadrature.net在英国就被Orange UK审查了数个星期。它被列入一个网站名单中，而近8年来Orange一直在拒绝承认这些网站。

可能是我们在反对这类立法时，提到了儿童色情这个词，也可能他们本来就讨厌我们，因为我们反对他们违背网络中立性[17]的政策，因为我们呼吁立法禁止他们对用户通信差别对待。我们永远不会知道。但是，服务商在这里扮演着这样一种角色，那就是他们在主动剥夺人们接触互联网信息的能力。无论我们把权力赋予Orange、政府，还是其他什么人，在这背后，我都看到了巨大的风险。

雅各布·阿佩尔鲍姆：请澄清一下，当你提到英国的隐私问题时，你的意思是不是他们真的握有每条线路、每条光纤连接和所有这些东西，或者他们利用了某些政府资源？广播是如何得到许可的？这里面到底有没有政府卷入？他们没有关注这件事的职责吗？

热雷米·齐默尔曼：这里有许可。无论是政府还是公司，他们在改变互联网的基本结构，把它从一个普遍的网络分割成像巴尔干地区那样的小型子网。但从一开始，我们讨论的就是全球性的事务，无论是金融系统的扭曲、腐败问题，还是地缘政治或能源环境问题。所有这些都是今天人类共同面临的全球性问题，而我们手上仍握有一个全球性的工具，可以实现更好的通信、更好的知识共享、更好的政治和民主参与。我怀疑，全球互联的普遍网络是我们应对这些全球性问题的唯一工具，因此争取一个自由的互联网是战斗的中心，我们所有人都有责任为此而战。

安迪·米勒–马贡：我完全同意我们需要确保互联网被理解为一个实现信息自由流动的普遍网络，我们不仅要明确这一点，而且也需要点明，某些公司和服务提供商，它们管它们提供的那种东西叫作互联网，而其实根本不是那么回事。但我认为我们还没有回答那个在过滤之上的关键问题。对于我认为我们需要回答的问题，我想给你举出一个例子。多年以前，我们发起过对西门子提供的所谓智能过滤软件的抗议。西门子是德国最大的电信公司之一，也是情报软件的供应商。他们真的在向公司出售这类过滤系统，例如，不让公司的雇员查看贸易工会向他们提醒劳工权益问题的站点，等等。但他们也封锁混沌计算机俱乐部的站点，这就惹怒了我们。他们把混沌俱乐部定为“犯罪内容”之类的东西，我们对此采取了法律措施。但是在一次展会上，我们决定发起一个大型的抗议集会，包围西门子的展台，对进出的人们进行过滤。好笑的是，

我们在自己的网站上宣布了这项行动，以便通过互联网吸引更多人参加，但西门子展台的人对此一无所知，因为他们自己也使用了这个过滤软件，所以读不到我们的公开警告。

朱利安·阿桑奇：五角大楼也设置了一套过滤系统，在寄给五角大楼的电子邮件中，所有带有维基解密字样的都会被过滤掉。所以在布拉德利·曼宁的案子中，控方为了起诉这个案子，当然要给在军事部门之外、与维基解密有关的人士发送邮件，但他们从未收到过回复，因为邮件中包括了“维基解密”这个词，于是被过滤掉了。[18] 国家安全体制也可能反噬自己。

安迪·米勒–马贡：这就把我们带回到这个基本问题：真的存在“负面影响信息”这类东西吗？从社会的视角看，我们是否想要一个受审查的互联网，因为这有利于社会？即便我们谈到儿童色情，你也可以争辩说：“等一下，儿童色情突显出一个问题，那就是对儿童的虐待，而为了解决这个问题，我们就需要了解它。”

雅各布·阿佩尔鲍姆：所以它必须提供犯罪的证据。

朱利安·阿桑奇：没有，它提供了一场游说。

安迪·米勒–马贡：这可能是最极端的例子：假如我们谈到纳粹之类的事，你仍然必须说出我们正在谈论的是什么。有家庭的人会扪心自问：“好吧，把坏事都过滤掉以便我们坚守好事，这是否更有利于社会？或者，这是不是在限制我们正视问题、管理问题、应对问题的能力？”

热雷米·齐默尔曼：我认为解决方案不会是审查。当我们谈到儿童色情，我们不应该使用色情这个词——它代表一种虐待儿童的犯罪行为。需要做的是去检查服务器，禁用服务器，识别出上传这些内容的人的身份以便识别出谁在制造这些内容、谁在第一现场虐待儿童。只要存在这种人际网络、商业网络之类的，你就能去逮捕这些人。当我们通过立法——在法国，我们有一部法律，你需要内政部部长的行政授权才能决定哪些网站要被封锁。通过说“我们消除了人们接触这些坏事的机会”，我们消除了调查部门去寻找坏人坏事的激励，就像我们用手去遮住那些发现问题的眼睛，然后我们就把问题解决了。所以，从这种角度看，我认为这样就足以描述这件事了——我们都同意我们应该把某些图片从互联网上删除。

雅各布·阿佩尔鲍姆：我很抱歉，这里我感到有点儿别扭。听到你这种论调太让人泄气了。你刚才说的有点儿恶心到我了，因为你等于是说：“我要利用我的职权去向其他人主张我的权威，我要擦除历史。”也许在这件事上我是个极端主义者——我敢说我在其他很多事情上也是——但这其实就是一个抹杀历史造成伤害的例子。它表明，通过互联网，我们知道社会上盛行着虐待儿童的现象。这就是我们从儿童色情的问题上所知道的——我认为管它叫儿童剥削更好——我们看到了它的证据。把这件事遮掩起来，抹杀它的存在，我认为就是一种歪曲，因为实际上你可以从一个作为整体的社会中得知如此多的事情。例如，你可以知道——显然，在我说这句话之后，我也永远不会去寻求参政，但只是澄清一下这点——例如，你知道了谁在制造它，你也知道了存在着受害者。人们不可能无视这个问题。这意味着你不得不开始寻找导致这个问题的原因，谁是儿童的剥削者。讽刺的是，在这里，某些监控技术有助于通过查看图片中的元数据识别出这些人的面部特征。擦除这些内容，让我们生活在一个可能擦除某些而不是另一些内容的世界，为了审查和监督而创建这些行政机构——正如我们所见，这会将我们引向一条危险的道路，其危险不仅在于版权，还包括很多其他系统。

正因为这是一项值得追求的高尚事业，我们也许就不该走捷径，也许我们确实就该去解决犯罪问题，也许我们确实应该试着去帮助那些受害者，即便为此需要付出代价。与其无视问题，也许我们应该正视事实，即社会作为一个整体存在着这个大问题，它以特定的方式显露在互联网上。

比如，这就像当宝丽来生产了Swinger拍立得相机（一种即拍即得的照相机），人们也开始用它来拍摄下流的照片。但对此的回应不是摧毁或监督这个媒介。当你要起诉这项犯罪，你就发现证据被这个媒介记录了下来。这并不会削弱这个媒介，也不会因这件事而损害全社会。

我们在这里谈到儿童色情，让我们谈到了监督。很多国家都存在骚扰人民的常规监督。在互联网上，警察所造成的伤害可能更甚于儿童色情。

朱利安·阿桑奇：几乎肯定更甚。

雅各布·阿佩尔鲍姆：我们知道在世界上有多少警察，但我们不知道其中有多少人违背了道德——通常是严重违背。比如，只要我们看一眼占领运动（the Occupy movement）[1]，我们就能发现。我们知道某些

警察有多坏，那么，我们就应该审查互联网吗？我们就应该削弱警察去执行良好监督工作的能力吗？

朱利安·阿桑奇：还有，这里有个二次伤害的问题，那就是当这个小孩长大成人后，通过社会联系，再次看到虐童的照片。

雅各布·阿佩尔鲍姆：只要那些警察还在网上，我就一直在遭受二次伤害。

朱利安·阿桑奇：你可以说，看见你被警察殴打的画面是二次伤害。我要说的是，保护世界上真实发生的历史的完整记录更为重要，就算二次伤害确实会发生，但是建立一个有能力移除大量历史的审查制度就意味着我们无法处理这些问题，因为我们根本看不到这些问题了。20世纪90年代，我在澳大利亚维多利亚儿童剥削行动组为打击猥亵儿童的警察提供互联网事务的咨询。那些警察并不喜欢过滤系统，因为一旦人们看不到互联网上有这些儿童色情，他们就不会去游说以从而确保警察得到打击虐待儿童的资金。

热雷米·齐默尔曼：有一点我们都同意，而且也认为这是最重要的一点，那就是，说到底，制造这些内容、虐待儿童或类似的事情，都是个人的责任，这是最要紧的，这才是警察应该解决的问题。

雅各布·阿佩尔鲍姆：我不同意，我不是这么说的。

朱利安·阿桑奇：热雷米说的是做这件事，不是说发表——这是两回事。

雅各布·阿佩尔鲍姆：说真的，内容的制造不是问题。稍微澄清一下——举例来说，你虐待了一个小孩，而安迪把这个拍下来作为证据，我不认为安迪就该为此被起诉。

热雷米·齐默尔曼：不，该被起诉的是那些实施虐待的人。但是拍摄也算协助与教唆。

安迪·米勒–马贡：但是有些人就是为了拍这些照片而虐待儿童的，对吧？

雅各布·阿佩尔鲍姆：当然有这种人。

安迪·米勒–马贡：这里可能还牵扯上经济问题。

雅各布·阿佩尔鲍姆：我完全同意，在这里我要做个区分，就是说内容本身是一份历史记录和一项罪证，是一项严重犯罪的证据，而且我们绝不能忽视二次伤害这件事，但是最初的伤害才是真正核心的问题，无论是否有这些照片。

热雷米·齐默尔曼：当然，这就是我的意思。

雅各布·阿佩尔鲍姆：是不是有这些照片几乎无关紧要。如果有这些照片，重要的是记住你必须关注的目标，是真正地去阻止伤害。重点要确保这些证据能激励人们正确地运用工具去解决问题。我认为这才是至关重要的，人们其实忘记了这一点，因为假装事情不存在太容易了，说是阻止了虐待而其实并没有。

安迪·米勒–马贡：而且麻烦在于很多人显然喜欢更轻松的解决方式，因为接受社会现实是很难的。我认为你确实有机会去处理政治问题，因为你并不是在试图制定一项忽视或者掩盖问题的政策。某种意义上说，这大概就是网络政治，但这也是一个社会如何处理事务的问题，我非常怀疑像信息这样的东西会造成直接的伤害。这确实与过滤的能力有关，那是当然，而且我也真的不想看到所有这些照片都被挂在互联网上。我确实发现有些东西是恶心和烦人的，但这对隔壁那家展示这种又假又难看的电影的音像店来说也是一样。所以，问题在于我是否有能力辨别自己的所见所闻？这就是一个过滤途径。其实，混沌俱乐部的创始人瓦乌·荷兰德（Wau Holland）说得好：“你要知道过滤应该由最终用户来决定，由终端用户的终端设备来执行。”[19]

朱利安·阿桑奇：所以应该是由那些接受信息的人来执行过滤。

安迪·米勒–马贡：过滤应该在这里执行。就在这儿！（指着他的脑袋）

朱利安·阿桑奇：在大脑中。

安迪·米勒–马贡：最终用户的最终设备——就是你两耳之间的东西，才是过滤的正当之所，过滤不该由政府代表人民来执行。如果人们不想看某些东西，那好，他们就不会看，而且，无论如何，现在也的确要求你自己去过滤很多事情。

注释

1．更多关于雅各布以及其余维基解密有关人士所遭到的骚扰，参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

2．参见维基解密关于Nadhmi Auchi的页面：http://wikileaks.org/wiki/Nadhmi_Auchi（访问于2012年10月24日）。

3．这些报道可以在维基解密上查到：http://wikileaks.org/wiki/Eight_stories_on_Obama_linked_billionaire_Nadhmsored_from_the_Guardian,_Observer,_Telegraph_and_New_Statesman（访问于2012年10月24日）。

4．一份一般性的记录可参见http://cables.mrkva.eu/和http://cablegatesearch.net，这里提供了对电报的完整版本和编改版本进行比较的精彩方法，由此可以看出维基解密的哪些媒体合作伙伴编改了电报。

5. “Qaddafi’s Son Is Bisexual and Other Things the New York Times Doesn’t Want You to Know”，载于Gawker，2011年9月16日，http://gawker.com/5840809/qaddafis-son-is-bisexual- and-other-things-the-new-york-times-doesnt-want-you-to-know-about；这个特例中所涉及的电报的参考号是06TRIPOLI198，载于维基解密：https://wikileaks.org/cable/2006/05/06TRIPOLI198.html。在Cablegatesearch网站可以直观地看到这些编改及其修改的历史记录，改编的段落都以紫色标记出来：http://www.cablegatesearch.net/cable.php?id=06TRIPOLI198&ver-sion=1291757400。（所有链接均访问于2012年10月22日）

6．原始电报参见电报参考号10STATE17263，载于维基解密：http://wikileaks.org/cable/2010/02/10STATE17263.html；《纽约时报》的报道参见“Iran Fortifies Its Arsenal With the Aid of North Korea”，载于《纽约时报》，2010年11月29日，http://www.nytimes.com/2010/11/29/world/middleeast/29missiles.html?_r=0。大卫·李（David Leigh）在给《卫报》的报道中也使用了同一份电报，“WikiLeaks cables expose Pakistan nuclear fears”，载于《卫报》，2010年11月30日，http://www.guardian.co.uk/world/2010/nov/30/wikileaks-cables-pakistan-nuclear-fears。这份电报的编改版本由《卫报》发布，并

且没有附上参考号，电报被缩减成只有两段关于巴基斯坦的文字。“US embassy cables:XXXXXXXXXXXX”，载于《卫报》，2010年11月30日，http://www.guardian.co.uk/world/us-embassy-cables-documents/250573。编改的程度可以在Cablegatesearch网站上直观地看到，并可以看到修改的历史记录，几乎整篇文件都被编改并以紫色标出：http://www.cablegatesearch.net/cable.php?id=10STATE17263&version=1291486260。（所有链接均访问于2012年10月22日）

7 . 原始电报参见电报参考号08KYIV2414，载于维基解密：http://wikileaks.org/cable/2008/12/08KYIV2414.html。《卫报》的编改版本参见“US embassy cables:Gas supplies linked to Russian mafia”，2010年12月1日，http://www.guardian.co.uk/world/us-embassy-cables-documents/182121?INTCMP=SRCH。编改版本可以在Cablegatesearch网站上直观地看到，并可以看到修改的历史记录，几乎整篇文件都被编改并以紫色标出：http://www.cablegatesearch.net/cable.php?id=08KYIV2414&version=1291255260。（所有链接均访问于2012年10月22日）

8 . 原始电报参见电报参考号10ASTANA72，载于维基解密：http://wikileaks.org/cable/2010/01/10ASTANA72.html.《卫报》的编改版本参见“US embassy cables:Kazakhstan-the big four”，载于《卫报》，2010年11月29日，http:// www.guardian.co.uk/world/us-embassy-cables-documents /245167?INTCMP=SRCH。编改版本可以在Cablegatesearch网站上直观地看到，并可以看到修改的历史记录，编改以紫色标出：http://www.cablegatesearch.net/cable.php?id=10ASTANA72&version=1291113360。（所有链接均访问于2012年10月22日）

9 . 这个事例中的电报参考号为09TRIPOLI413，这份电报是关于西方能源公司在利比亚的经营活动。在Cablegatesearch网站可以直观地看到《卫报》的改编被以紫色标出，其中显示，《卫报》删除了所有被提到的能源公司及其经理的名字，除了一家俄罗斯能源公司Gazprom。即使那些无损于西方公司的内容也做了精心编改，而编改的版本给出一幅完全不同的画面：http://www.cablegatesearch.net/cable.php?id =09TRIPOL I413&ver-sion=1296509820（访问于2012年10月22日）。

10 . 这个事例中的原始电报包含了5226个单词，而《卫报》发布的

改编版本只有1406个单词。原始电报参见电报参考号05SOFIA1207，载于维基解密：http://wikileaks.org/cable/2005/07/05SOFIA1207.html。《卫报》的改编版本参见“US embassy cables:Organised crime in Bulgaria”，2010年12月1日，http://www.guardian.co.uk/world/us-embassy-cables-documents/36013。基于这份电报的《卫报》报道，参见“WikiLeaks cables:Russian government ‘using mafia for its dirty work’”，载于《卫报》，2010年12月1日，http://www.guardian.co.uk/world/2010/dec/01/wikileaks-cable-spain-russian-mafia。编改的程度可以在Cablegatesearch网站上直观地看到，并可以看到修改的历史记录，编改以紫色标出：http://www.cablegatesearch.net/cable.php?id=05SOFIA1207&version=1291757400。维基解密的保加利亚媒体合作伙伴Bivol讨论了这个保加利亚的事例，见“Unedited cable from Sofia shows the total invasion of the state by organized crime (Update:Cable Comparison)”，载于WL Central，2011年3月18日，http://wlcentral.org/node/1480.亦可参见“The Guardian:Redacting,censoring or lying?”，载于WL Central，2011年3月19日，http://wlcentral.org/node/1490。下面这两条WL Central的报道是《卫报》记者大卫·李的评论和回应。（所有链接均访问于2012年10月22日）

11 ．这里提到的电报的参考号是09BERLIN1108。编改版本可以在Cablegatesearch网站上直观地看到，并可以看到修改的历史记录，编改以紫色标出：http://www.cablegatesearch.net/cable.php?id=09BERLIN1108&version=1291380660（访问于2012年10月22日）。

12 ．更多事例参见cabledrum网站：http://www.cabledrum.net/pages/censorship.php。

13 .“通信拦截。主席提供了关于事情进展的信息……它回顾了媒体关于此问题的负面报道……在此背景下，主席认为此事进展甚慢……某些代表在准备新闻稿时表现出谨慎态度，指出这会引发连锁反应并加剧媒体的负面报道。本委员会对此立场不变，并向这些代表指出，一种打破僵局的可能途径是采取与处理互联网儿童色情问题类似的策略。尽管需要承认这是不同的问题，但它也涉及通信拦截。”——欧盟委员会，关于通信拦截的警察合作工作组会议（Police Co-operation Working Group meeting on interception of telecommunication），1999年10月13—14日。全文见：http://www.quintessenz.at/doqs/00010000

2292/1999_10_13,Police%20Cooperation%20Working%20Group%20mixed%20committee%20meeting.pdf（访问于2012年10月24日）。

14 ．参见讨论之前的“对维基解密及相关人员的各种迫害企图的注释”。

15 ．雅各布所说的吉尔莫诉司法部部长冈萨雷斯案，35 F.3d 1125（2006年第九巡回法院）［Gilmore v.Gonzales,435 F.3d 1125（9th Cir.2006）］。约翰·吉尔莫原本是一位密码朋克，他提出这个案子，最终使得美国最高法院曝光了一条秘密法的内容，这条秘密法叫作安全指令（Security Directive），该法限制公民匿名乘坐飞机旅行的权利。除了违背宪法之外，吉尔莫还质疑这样一个事实，那就是这项条款本身就是秘密的、不能曝光的，即便它已经对美国公民构成了约束。法院秘密查阅了安全指令，否决了吉尔莫对该条款违宪的指控。但是，这条法律的内容却在案件审理过程中被曝光出来。参见PapersPlease.org上吉尔莫诉司法部部长冈萨雷斯案的报道：http://papersplease.org/gilmore/facts.htm（访问于2012年10月22日）。

16 ．克里斯钦尼亚是位于丹麦哥本哈根的一片自行宣布的自治地区。这里从前是一片军营，在20世纪70年代被一群泛集体主义者和无政府主义者占领。它在丹麦创造了一种独一无二的法律地位。

17 ．“网络中立性”（Net neutrality）原则要求从法律上保障ISP不得限制其用户接入网络、参与互联网活动，也不得限制访问网上的内容。参见电子前哨基金关于网络中立性的页面：https://www.eff.org/issues/net-neutrality（访问于2012年10月24日）。

18 ．“Blocking WikiLeaks emails trips up Bradley Manning prosecution”，载于Politico，2012年3月15日，http://www.politico.com/blogs/under-the-radar/2012/03/blocking-wikileaks-emails-trips-up-bradley-man-ning-117573.html（访问于2012年10月21日）。

19．更多关于瓦乌·荷兰德（Wau Holland）的信息参见瓦乌·荷兰德的主页：http://www.wauland.de。

[1] 起源于2011年的占领华尔街的集会示威活动，后来发展成全球抗议。——译者注

弱者要隐私，强者要透明

朱利安·阿桑奇：安迪，最近我跟突尼斯总统谈话，我问他会怎么处理本·阿里独裁统治时期留下的情报记录，这些记录相当于突尼斯版的斯塔西档案 [1] 。他说虽然情报非常有趣，但这些情报机关却是个麻烦，它们太危险了，必须逐个把它们撤销掉。但对于那些档案，他认为，为了维护突尼斯的社会团结，最好把它们全面封存，这样才不会导致各种推卸责任的局面。斯塔西在民主德国失势时，你还是个年轻人，你能说一说斯塔西档案的事吗，还有你是怎么看待秘密档案的公开的？

安迪·米勒–马贡：德国也许拥有这个行星上档案记录最为完善的情报机构，至少也是其中之一。民主德国国家安全局的所有档案，包括所有手册、程序文件、训练文件、内部学习资料，几乎全都公开了。几乎的意思是说，并不是所有文件都能轻易搞到，但大部分很容易，而且，政府还成立了一个机构来看管这些记录，所以德国公民也有权阅读他们自己的斯塔西档案。

朱利安·阿桑奇：民主德国政府成立了联邦国家安全档案委员会来处理巨量的斯塔西档案。

安迪·米勒–马贡：是的，记者可以申请所谓的调查研究，这有点儿类似于信息自由询问权，这允许他们研究这些材料。有大量的书籍，还有关于战术训练的手册，从中能够看出斯塔西是如何运用这些手段的。实际上，我认为这是一件值得学习的事。我理解要求突尼斯人公开所有这些前情报机关留下的个人记录是奢望，因为现任总统将会评判他自己及其盟友们的记录。这些情报机关毫不尊重隐私，所以你可能会看到关于你的性生活的记录，你的电话通讯录、你的财务转移记录，以及所有你做过的事情的记录，其中也许就有你不愿曝光的。

朱利安·阿桑奇：你关注了与Amn El Dawla有关的局势吗，那个埃及的国内安全机关？数千人闯进去，洗劫了档案库，因为Amn El Dawla试图烧毁这些档案，把它们都扔进垃圾堆，很多材料流传出来，在周边散播。你在当地市场花2美元就能买到一份记录并把它上传，埃及社会也并未因此毁灭。

安迪·米勒–马贡：不，我只是在说我确实有点儿理解人们并不愿意自己的个人记录被公布。我能够理解这点，如果我生活在这样一个国家，情报机关40年来都在监视我，我每次上厕所都会被记录。

朱利安·阿桑奇：但是这里有一个成本收益分析，对吧？依我之见，一日做贼，终身为贼。

安迪·米勒–马贡：对，但黑客伦理一般主张利用公开信息，保护私人信息，而且，我确实认为，如果我们在倡导隐私保护——我们有非常正当的理由这么做——那我们就不应该只是说这里有利益权衡。我们要做出区分。事情并不要求我们把一切都公之于众。

雅各布·阿佩尔鲍姆：但是这种不对称的保密有一个好处。让我们退一步讲，你的论证基本上基于一个完全错误的观点，那就是，只要数据是受限的，那它就是私密的，但这并不是事实。举例来说，在我的国家，如果有100万人得到安全许可并被允许获取私人数据……

朱利安·阿桑奇：是430万人……

雅各布·阿佩尔鲍姆：那你怎么能说这些数据是私密的？问题是这些数据并不是对这个世界上的所有人都是百分之百保密的。

朱利安·阿桑奇：秘密从没有权力的人那里被转交到有权有势的人那里。

安迪·米勒–马贡：对，你说得对。但如果我们想完全公开整个档案库。

朱利安·阿桑奇：在某些欧洲国家就是这样。

安迪·米勒–马贡：不对，我不知道有哪一个国家是将所有记录都公开的。

朱利安·阿桑奇：比如波兰，公开记录的程度就比德国高。

安迪·米勒–马贡：也许吧。实际上发生了什么，德国所做的这笔交易中不好的一面是他们雇用了前民主德国国家安全局的官员，他们不仅管理斯塔西的记录，还包括所谓的“新德国”，即统一后的前民主德国部分的记录。这里有一个非常有趣的故事，一家公司赢得了公开招标去清

理一幢保存着记录的建筑。这家公司赢得招标的原因只是他们是报价最低的投标者。六年之后，保管这些记录的组织发现他们雇用了一家由前民主德国情报机关人员建立起来的公司来清理他们自己的记录。

热雷米·齐默尔曼：维基解密上有一份关于这件事的报道。我读过，非常精彩。[1]

安迪·米勒–马贡：维基解密发布了这份报告，所以你是对的，一旦这些记录被创造出来，并且落在坏人手中，就很难宣称这些记录是私密的。

朱利安·阿桑奇：但是我们可以谈一谈一个广泛的问题。互联网导致了一场信息爆炸，海量数据得以公开——这是非常惊人的，而它的教育功能也是惊人的。

一方面，人们谈到维基解密，他们说："看啊，政府的所有私密信息现在都被公开了，政府不再掌握任何秘密了。"我说，这是废话。我说，维基解密是影子的影子。事实上，我们向公众发布的超过100万字的信息只是海量秘密材料的一小部分。而且，事实上，相比权势集团掌握的海量秘密材料，公开可得的材料相形见绌，而维基解密所公布的还只是这些私人持有的材料的百分之一。当你一边看着有权有势的局内人清楚全世界每一张信用卡的交易信息，另一边看到人们在Google上搜索全世界的博客和人们的留言，那么你如何能看得到平衡呢？

安迪·米勒–马贡：我想说，如果所有这些记录都能得到披露，那很好，因为人们可以学到，当他们使用信用卡时，他们留下了痕迹。如果我们把这些解释给某些人听，他们会发现这是非常难以理解和抽象的东西。但当他们读到自己的记录的那一刻，他们就全明白了。

朱利安·阿桑奇：如果你得到你的Facebook记录，其中关于你的信息就有800MB。

安迪·米勒–马贡：我知道东欧集团覆灭后，联邦德国总理赫尔穆特·科尔想要统一德国，美国人想在所谓的2+4会谈中设置一项条件。美国人想要保持对德国电子通信的控制和监控，而科尔觉得无所谓，因为他不理解什么是电信监控。我遇到过他办公室的一些人，他们说，他们对此简直要抓狂了，最终，他们组织起来，从斯塔西那儿搞来8000页他的电话通话文字记录，塞进两辆小卡车运到他的办公室。然后他

问：“嘿，这都是什么该死的玩意儿？”他们说：“哦，这是您过去十年间的通话记录，包括您跟您的女友、妻子，还有秘书的，等等。”于是，他们让他明白了电信拦截意味着什么。而且，这些来自情报机构的记录确实能够帮助人们了解情报机构都在做什么。所以，我们可以力争全面披露，而且如果我们现在就对此投票的话，我不确定自己是否真会反对它。

朱利安·阿桑奇：我不想过多谈论这个了，因为在某些情况下这是显而易见的，如果你在调查黑手党，那么在调查期间，你应该对你的记录保密。在这种情况下保密是合情合理的。我不是说作为一项政策这是合理的，我说的是，这在政治上是不可避免的。有很多这类在政治上强有力的要求，像是“这些家伙曾经杀过人，他们也许在密谋下一桩谋杀”——不管认为拦截是否应该，这都会发生。你不可能赢得这场政治斗争。但是这类战术监控，如果能够受到部分监管，并把伤害的人群减小到最低限度，那还是有好处的。当战术监控用于加强执法（与情报机关相对），它常常是证据搜集的一部分。这些证据最终会呈交法庭，因而最终也会公之于众。所以，至少在某些时候，你能够对正在发生的事情有所监督。你可以在听证席上质问人们这些信息是如何搜集到的，以及我们为何应该假设这些证据是有效的。你对此可以密切监督。但是对战略监控的所谓管制就完全是荒谬的了。根据定义，战略监控是在监控所有人，如果你的前提就是监控所有人，那么我们能够向何种法规申诉呢？

热雷米·齐默尔曼：关于全面披露的辩论让我想起一个叫作LulzSec的团体，他们公布了7000万份来自索尼公司的记录——所有索尼客户的数据——你可以看到所有地址、电子邮箱和密码。我觉得里面甚至有这7000万用户的信用卡明细。作为一个倡导基本人权的积极分子，我想：“哇哦，如果为了证明你的观点，或就为了好玩，你就要曝光别人的个人数据，这里一定有什么不对。”看到记录中有人们的电子邮箱，我感到非常不舒服。某种程度上，我觉得这些人就是在利用计算机安全来取乐，但他们所展示的是，像索尼这样声名狼藉又财大气粗的公司也不能为用户的私密信息保密，还让这7000万用户的电邮、姓名在一个搜索引擎上就能被检索到。发现这些记录可能让人们立马意识到：“哦，当我把这些数据暴露给索尼时，我都做了什么？将个人数据交给一个公司保管到底意味着什么？”

雅各布·阿佩尔鲍姆：然后他们就向报信的人开火了。

注释

1 . “Stasi still in charge of Stasi files”，载于维基解密，2007年10月4日，http://www.wikileaks.org/wiki/Stasi_still_in_charge_of_Stasi_files（访问于2012年10月22日）。

[1] 斯塔西从1950年起对社会进行持续监控，搜集并建立了海量的个人档案库。1990年12月，德国国会通过《斯塔西档案法》，赋予查阅档案的法律依据。1992年起，斯塔西档案正式向外界开放查阅。——译者注

歌剧院里的耗子

朱利安·阿桑奇：我们已经谈过了所有这些悲观的场景，现在我想来看一看一种潜在的乌托邦场景。我们已经有了一代激进的互联网青年，现在这些人正在成为年轻人中的大多数。另一方面，我们也在匿名化、出版自由和逃避审查方面做着绝望的斗争，太多的政府和私人部门勾结起来对抗我们的努力，但是，让我们做个最积极的假设，看看事情会变成什么样子。

雅各布·阿佩尔鲍姆：我认为我们需要有自由阅读和自由发言的权利，并将这种权利惠及每一个人，没有一个人被排除在外，没有任何例外，这里我可以借用比尔·希克斯（Bill Hicks）的话。[1]这是他在谈到教育、衣服和食物问题时表达的看法，但用在这里也是恰当的。每个人都有权自由地阅读，每个人都有权自由地表达。同样的道理也适用于匿名发言的权利，让人们能够不受第三方干扰地进行支付，让人们能够自由地旅行，让人们能够在系统中纠正关于自己的信息。让我们所看到的各种机构的系统都变成透明和可问责的。

安迪·米勒–马贡：我想要再加一个观点，那就是随着信息处理系统及网络的增加，随着像Tor和加密技术这样的工具的出现，能够被压制的信息的数量已经变得相当少了，这意味着政府也知道他们只需要做这些事了。他们知道，在今天，秘密行动仅仅意味着能在一段时期内将行动保密，这些行动迟早都是要公之于众的，这是件好事。这改变了他们的行为方式。这表明他们也知道要对自己的行为负责。这也意味着他们将告发活动强加进了事情的进程当中，就像《萨班斯法案》（Sarbanes-Oxley Act）要求在美国股市注册的公司具有告发的机制，以便让想告发犯罪行为和上司的不端行为的人可以有告发的渠道，而不必受到他们所告发的人的直接阻扰。[2]所以，这是件好事，这会在长期中带来更具有可持续性的进程。

热雷米·齐默尔曼：对雅克刚刚所说的再做一点补充，我认为，我们必须让每个人都明白这一点，一个自由、开放、普遍的互联网可能是我们处理关键的全球性问题的最重要的工具，我们这一代人最重要的任务之一，可能就是保护这种互联网，将它置于我们的掌握之中。一旦某

方面的力量——无论是政府势力还是公司势力——要限制某些人接触这种普遍互联网的能力，整个互联网都会受到影响，整个人类都会受到限制。正如我们正在见证的，我们能够依靠集体行动来增加这种决策的政治成本，所有访问自由互联网的公民都能阻止这种行为。我们开始意识到，作为互联网公民，我们在政治决策中有这样的权力，我们可以让我们选出的代表和我们的政府对他们的所作所为更加负责，特别是当他们做错事时，当他们损害了我们的基本自由时，当他们损害了这种自由的全球普遍互联网时。

所以，我们应当把这些想法付诸实践。我们应当继续分享这种知识，教会人们如何实践这些想法。我们应当继续改善我们的行动方式，交流关于走进议会的策略，曝光政客们的所作所为，披露工业游说集团在政策制定过程中的影响。我们应当继续开发工具，让公民们更有能力去建造他们自己的去中心化加密基础设施，拥有他们自己的通信基础设施。我们应当向全社会推广这种观点，这种建立一个更好的世界的方式，而且，我们也正在开始这样做，我们只是应当继续努力。

朱利安·阿桑奇：雅克，如果你看一下叶夫根尼·莫洛佐夫（Evgeny Morozov）对互联网问题的描述，你就会发现，这些问题是多年以前密码朋克早就预见到的。[3] 这种观点认为，人们对新兴的监控状态不能仅仅是抱怨一下，事实上，我们能够开发出一种新的民主工具。事实上，我们能够运用我们的智慧开发出这些工具，将这些工具散发给其他人，促成集体防御。技术和科学并不是中立的。某些特定形式的技术可以带给我们基本权利和自由，而这些权利和自由是许多人长久以来所渴望的。

雅各布·阿佩尔鲍姆：完全正确。我认为关键是人们应该走出来，特别是那些十六七岁的年轻人，如果他们希望建设一个更好的世界的话。没有人是坐在家里就能把事情办成的，世界上也从来没有人一出生就带着将来能刻在他们墓碑上的成就。我们所有人都要创造更多的选择。在座的各位都在创造这种替代选择，特别是通过互联网，每个人都有权为他们自己的生活环境做出更多的创造。这里并不是说他们有义务进行这种创造，而是说，如果他们愿意，他们就能够这么做。而一旦他们这么做了，势必会影响更多人，特别是在互联网上。这种对替代选择的创造具有一种放大效应，会得到不断增强。

朱利安·阿桑奇：所以，就算你只是为了自己使用而创造了什么东西，你也可以把它提供给数十亿人使用。

雅各布·阿佩尔鲍姆：或者说，一旦你参与匿名网络的开发，就像Tor这样的网络，你就帮助建立了一种前所未有的匿名通信的替代选择。

热雷米·齐默尔曼：这是关于自由分享知识的问题，也是提供一种可供知识自由分享的通信渠道的问题，这就是你正在从事的工作。Tor是一个在今天得到广泛传播的自由软件，因为我们将自由的观念内置到我们建立替代选择、开发技术和模型的方式中。

雅各布·阿佩尔鲍姆：一个自由的社会需要自由的软件，我们也需要自由和开放的硬件。

朱利安·阿桑奇：说到自由，你指的是不受束缚吗？人们可以捣鼓内部结构，看看它是如何运行的？

雅各布·阿佩尔鲍姆：就是这个意思。我们需要自由的软件，就像民主制度需要自由的法律，在民主制度中，每个人都能够学习法律、修改法律，能够真正地理解法律并确保法律得到如期执行。所以我们也需要自由的软件，自由且开放的硬件。[4]

朱利安·阿桑奇：这是密码朋克的一个观念吧，“代码即法律”（Code is law）。

热雷米·齐默尔曼：这是拉里·莱斯格的观点。

朱利安·阿桑奇：在互联网上，你能够做什么是由现存的程序以及程序的运行所定义的，因此可以说代码就是法律。

雅各布·阿佩尔鲍姆：确实如此，这也意味着你可以创造替代选择，特别是通过编程，甚至通过3D打印或其他在黑客世界中存在的社会工具。[5]你可以帮助创造替代选择，而关键在于使其成为一种常规行为，人们会变得非常习惯于创造他们自己的三维物品，以及改编自己的软件，这会成为一种社会习俗；而且，他们会意识到，那些阻碍他们这么做的人根本不是在提供互联网，而是在制造障碍，他们所提供的只是一种过滤网（filternet）或审查网（censornet），而非互联网，事实上，他们违背了他们照看互联网的职责。

这就是我们每个人每天所从事的工作，人们应该知道他们有能力这么做，既为了子孙后代，也为了当代的同胞。这就是我来这里的原因，因为如果朱利安正遭受这样的待遇，而我现在不出来支持他，那我又是在建立怎样的世界呢？当我让自己被一群猪猡任意摆布，我又是在传递怎样的信息呢？没门儿，我绝不会让他们得逞！我们必须去建设，我们必须去改变。正如甘地所说，“你希望看到世界有所改变，必先改变自己”，但是，你希望看到世界有麻烦，也必先使自己成为那种麻烦。[6]这是《一个更温柔的世界》（*A Softer World*）中的一段话，与甘地的名言并不完全一致，但我认为人们需要知道他们不能只是懒散地坐着，他们需要采取实际行动，但愿他们能这么做。[7]

安迪·米勒–马贡：我认为我们正恰逢一个很好的机遇，人们会从我们这里出发，进一步推动事情发展，那些对现状或现存选择不满的人会去创造替代的选择。

朱利安·阿桑奇：你能在这种背景下谈一谈混沌计算机俱乐部的作用吗？

安迪·米勒–马贡：总是会提到混沌俱乐部……fnord[8]。

朱利安·阿桑奇：因为它确实是世界上独一无二的。

安迪·米勒–马贡：混沌俱乐部是一个巨型的黑客组织，致力于推广信息自由、技术透明的理念，同时也关注人类与技术发展之间的关系，以及社会与发展的互动关系。

朱利安·阿桑奇：这些实际上都是政治问题。

安迪·米勒–马贡：混沌俱乐部有点儿像一个黑客现场论坛，大概有数千名会员，基本上都在德国，但是我们不认为自己生活在德国，我们认为自己生活在互联网上，这是我们自我认知的一大部分，也是很诱人的一部分。我们与其他一些位于法国、美国以及世界其他地区的黑客团体也保持着良好的联系。

朱利安·阿桑奇：那么，你认为为什么它会起源于德国？它以德国为核心，并扩张到世界的其他地区。

安迪·米勒–马贡：德国人总是试图把每一件事都组织化。

热雷米·齐默尔曼：德国人的工程学更好。

朱利安·阿桑奇：但是我觉得不只是因为这个。它位于柏林，位于没落的民主德国。

安迪·米勒–马贡：这与很多事情都有关系。德国作为一个国家，对其他国家做了最糟的事，所以，也许德国对重蹈覆辙多少有点儿免疫了，像是对其他国家发动战争这类事。我们从前都干过，我们从前都经历过，我们也遭到了严厉的惩罚，我们不得不从中吸取教训。而且，实际上，德国的学校现在还在教导这种去中心化的思维方式和反法西斯的行为，就是为了避免成为一个极权主义国家，因为我们曾经历过最糟的状况。所以，我觉得这也是理解混沌俱乐部的一个方面：这是一种德国现象。混沌俱乐部的创始人瓦乌·荷兰德对此也有一种强烈的政治倾向。我在他的墓前见过他父亲，白发人送黑发人，父亲当然说不出什么高兴的话。他只是说：“从此以后，在德国的土地上，再也不会发生任何极权主义的、非和平的行为了。”这就是他的父亲在埋葬自己的儿子时说的话。对我来说，这在很大程度上解释了为什么瓦乌会如此投入到他的事业中：影响和照顾他人，与他人和平相处，传播而不是限制理念，协同合作而不是独断专行。

而且，这种创造性合作的思想，就像开源运动一样，深深地影响了其他思想，并与美国赛博朋克的思想，以及朱利安·阿桑奇和维基解密所代表的思想一起出现。这是一种全球性的事物，但又带有瑞士、德国、意大利黑客各不相同的、高度去中心化的文化态度，这很好。意大利黑客的行事方式与德国黑客的完全不同，无论他们到哪儿，他们都需要做好吃的，而德国黑客则需要让每件事情都井然有序。我不是说一种方式就比另一种更好，我只是说这些去中心化的文化中的每一种都有其自身的优点。在意大利的黑客大会上，你还能去厨房，你会看到一个非常奇妙的地方；在德国的黑客营地，你可以享受非常棒的互联网，但最好别去看厨房。但事情的核心还是我们在进行创造。而且，我认为，我们发现自己拥有了某种共同的意识，这完全不同于对国家的认同，无论是德国人还是意大利人，或是法国人或其他什么国家的人，这都无所谓，我们只是看到我们都想解决问题，我们都想携手工作。我们看到了互联网审查，这是政府在与新技术作对，我们必须克服这种变局。

我们不仅在发现问题，也在寻找解决之道，这是件好事。也许我们还得被迫跟这些垃圾对抗不知道多少年，但是现在终于出现了这样一代政治家，他们不会把互联网视为敌人，他们明白了互联网并非问题的一

部分，而是解决之道的一部分。我们的世界仍旧建立在武器之上，建立在秘密权力之上，建立在一个总体经济框架之上，但是事情也在发生变化，而我真的认为我们在现在的决策制定中会起到非常重要的作用。我们可以通过一种有争议的方式来讨论问题，就像混沌俱乐部长久以来所做的那样。我们并不是一个同质化的群体，我们有许多不同的意见。我明白，我们在这里坐在一起，也并不会马上就得出最好的答案，我们只是在提出问题，把各自不同的观点摆到桌面上，让观点发生碰撞，看看底线是什么。这个过程需要持续下去，我们需要一个自由的互联网来推动这种讨论 .。

朱利安·阿桑奇：我抛出了这个问题：看看未来世界的最积极方向是什么样子。那就是自我认知、多样性和自决的网络。受过高等教育的全球人口——我不是指正规教育，而是说他们对人类文明在政治、工业、科学和心理等各个方面的运作方式都有高度的理解——是自由交流的产物，这同时也刺激了新文化的茁壮发展，以及个人思想最大限度的多样化，增加了地区的自决、利益集团的自决，同时能促进快速的联合以及超越地理限制的迅速的价值交换，就像“阿拉伯之春”和泛阿拉伯运动中所展现的那样，那些运动都是通过互联网才成为可能的。Nawaat.org创建了Tunileaks，并突破了当局的审查，促进了美国国务院的电报进入到革命前的突尼斯。在我们与他们的合作中，我们目睹了互联网的巨大能量，把信息传递到任何需要它的地方，正是因为我们的努力，我们才取得了巨大的回报，并对那里正在启动的改革做出了贡献。[9]我不觉得这种争取自决的斗争与我们自己的斗争有何不同。

最积极的方向必将要求对人类文明的自我认知，因为历史是不容毁灭的。这意味着新的极权主义国家在现实中不可能再出现了，因为信息的自由流动，人们能够私下交流，能够进行反对那种趋势的密谋，微型资本也能够逃离那些不适宜人类活动的地方的控制，得以自由流动。

在这些基础之上，你可以建立各种各样的政治体系。如果只有一个乌托邦，那这个乌托邦对我来说就是个反乌托邦。我认为乌托邦的理想必须意味着体系和互动模式的多样性。你看一看新文化产品、语言的演变和亚文化的躁动和发展，这些事物都形成了各自的互动机制，而这又是因为互联网而成为可能的，那么我就可以说，是的，这确实打开了可能的积极道路。

但是，在所有那些趋向同质化、普遍化的可能性中，整个人类文明最终会变成只有一个市场，这意味着，对于每一种服务和每一种产品，

你都只能拥有常规的市场要素，例如一个市场领导者，一个老二，一个第三位捡漏的选手，然后就是些毫无用处的散兵游勇。我认为这将导致大范围的语言同质化、大范围的文化同质化，以及大规模的标准化，这样才能够让那些快速交易变得更有效率。所以，我认为这种悲观的场景也是非常有可能出现的，而跨国监控和无穷无尽的无人机战争也会落到我们头上。

实际上，我倒想起了一件事，有一次我偷偷溜进悉尼歌剧院，去看《浮士德》。悉尼歌剧院在晚上看起来非常漂亮，它有壮观的内部装饰，灯光闪耀在水面上，照亮了夜空。然后，我来到外面，听见三位女士正在聊天，她们倚着栏杆，俯瞰着黑色的港湾。有位年长的女士在描述她在工作中遭遇的困难，最后我发现她是为中央情报局服务的一名情报官，她以嘶哑的腔调向她的侄女和另一位女士讲述她之前对美国参议院情报委员会（Senate Select Committee for Intelligence）的抱怨。我想："所以这是真的了。中央情报局的官员真的在悉尼歌剧院里晃荡！"然后，我又仔细观察了一番歌剧院的内部，透过正面宏伟的玻璃幕墙，我看到一切都是那么幽静、平和、精致，但在这当中，有一只耗子从水面爬上来，进入了歌剧院内部，这耗子在铺着亚麻布的桌子上蹿来跳去，啃咬剧院里的食物，跳上满是戏票的柜台，享受着这美妙的时刻。而这让我想到，这就是未来最有可能出现的场景，一个极其狭隘、同质化的后现代跨国极权主义体系，这个体系具有非凡的复杂性、荒谬性和低俗性，在这种非凡的综合体中，唯有那些聪明的耗子才能自由活动。

这就是消极的方向上的一个积极角度，这种消极的方向通往跨国监控、无人机攻击和跨国精英的新封建主义关系网。这种关系网并不是传统意义上的，而是各行各业的精英组成的，他们从自己的民族国家中超脱出来，脱离他们的民众基础，相互勾结，结果是形成了一种复杂的多党互动。所有的通信都将受到监控，并被永久记录、永久追踪，从出生到老死，每一个个体的所有互动活动都会在新体制中被永久识别。这就是过去十年来的主要趋势，我们实际上已经处在这种局面之中了。我认为，这种局面只会造成一种非常压抑的氛围。如果所有搜集到的关于世界的信息都能得到公开，就能对权力运动形成制衡，并让作为一个全球文明的我们，能够塑造自己的命运。但是，除非发生剧烈的变动，这种情况不会发生。大规模监控正在压倒性地作用于我们中的大多数人，而将权力不成比例地转移给那些谋划这种局面的人。尽管我认为这些人也不会享受这种美丽新世界。这种体系也将与无人机军备竞赛结合到一

起，并消除我们所知的明确划分的边界，因为这种边界是由于物理断裂带上的竞争而产生的。这将导致一种永久性战争状态，因为获胜的影响力关系网正开始动摇世界，要求世界做出妥协。与此同时，人们将葬身于无可解脱的官僚制强压中。

一个普通人如何能在这样的体系中得到自由呢？根本不可能，这是不可能的。在任何体系中，任何人都不可能获得完全的自由，但是，我们作为生物进化而来的这些自由，我们作为文明所习惯了的这些自由，几乎将会被这种体系彻底毁灭。

所以，我认为，只有那些在这个体系的内部受到过高等教育的人，能在未来保住这种我们在二十年前曾享有过的自由，因为监控状态已经把大部分自由都彻底毁灭了，我们根本无法再意识到这种监控的存在。所以，可能只有高技术的反叛精英才是自由的，那些在歌剧院里跑来跑去的聪明耗子。

注释

1．“你在这里所能做的就是改变世界，就是现在，让世界朝着更好的方向发展。把我们每年花在军备和国防上的钱都用来为世界上的穷人生产食物、提供衣服和教育，把所有人都包括在内，这样我们就能够一起探索太空，探索我们内在和外在的世界，并永远生活在和平中。”——比尔·希克斯，此话出自一段视频“Bill Hicks - Positive Drugs Story”，http://youtu.be/vX1CvW38cHA（访问于2012年10月24日）。

2．2002年的《萨班斯—奥克斯利法案》（The Sarbanes-Oxley Act）是美国为回应安然（Enron）、泰科国际（Tyco International）、阿德菲亚（Adelphia）、百富勤系统（Peregrine Systems）和世通（WorldCom）的公司会计丑闻而通过的一部法案。该法案的目的是消除会导致这些危机的同类腐败行为。该法案的1107条被编入美国法典1513（e）［USC 1513（e）］，将报复告发者的企图视作一种犯罪行为。

3．叶夫根尼·莫洛佐夫的《网络错觉：互联网自由的黑暗面》（*The Net Delusion:The Dark Side of Internet Freedom* , Public Affairs, 2011）。

4．关于自由软件，参见GNU操作系统网站上的“The Free Software Definition”：https://www.gnu.org/philosophy/free-sw.html。自由硬件指的

是不受制于专利知识产权的硬件，这种硬件以公开的标准建造，这里不存在打击逆向工程或篡改的法律（也没有反规避法），硬件设计的原则、指南和方案都是自由获取的，这样一来，任何人都可以拥有这种硬件以及建造副本的必要资源。更多关于自由硬件的信息参见“Exceptionally Hard and Soft Meeting:exploring the frontiers of open source and DIY”，载于EHSM：http://ehsm.eu。亦可参见维基百科上的“Open-source hardware”：https://en.wikipedia.org/wiki/Open-source_hardware。（所有链接均访问于2012年10月24日）

5 . 关于使用自由和开放的硬件进行3D打印的信息，参见RepRap 3D打印机的一段介绍视频：http://vimeo.com/ 5202148（访问于2012年10月24日）。

6 . “成为你所希望看到的世界中的麻烦”（Be the trouble you want to see in the world）语出《一个更温柔的世界》（*A Softer World* ），这是一个网络漫画刊物：http://www.asofterworld.com/index.php?id=189（访问于2012年10月24日）。

7 ． 想要进一步了解这段讨论中的相关问题，雅各布推荐以下两个书目资源：“匿名书单”（The Anonymity Bibliography），关于匿名的论文精选，由罗杰·丁格勒戴和尼克·马修森管理：http://freehaven.net/anonbib；“审查书单”（The Censorship Bibliography），关于审查的论文精选，由菲利普·温特（Philipp Winter）管理：www.cs.kau.se/philwint/censorbib。（两个链接均访问于2012年10月24日）

8 . fnord代表句子中故意留下空白。

9 ． Nawaat.org是一家独立的集体博客，于2004年在突尼斯创建：http://nawaat.org/portail。Tunileaks由Nawaat于2010年11月创建，它发布了维基解密上有关突尼斯的电报：https://tunileaks.appspot.com。更多关于Tunilinks以及本·阿里政府对其采取的审查行动的信息，参见“Tunisia:Censorship Continues as Wikileaks Cables Make the Rounds”，载于Global Voices Advocacy，2010年12月7日，http://advocacy.globalvoicesonline.org/2010/12/07/tunisia-censorship-continues-as-wikileaks-cables-make-the-rounds。（所有链接均访问于2012年10月24日）

图书在版编目（CIP）数据

密码朋克：自由与互联网的未来 /（澳）朱利安·阿桑奇著，Gavroche译. -- 北京：中信出版社，2017.10
书名原文：Cypherpunks:Freedom and the Future of the Internet
ISBN 978-7-5086-7624-1
I. ①密… II. ①朱… ②G… III. ①密码－加密技术－研究 IV. ①TN918.4
中国版本图书馆CIP数据核字（2017）第108263号

密码朋克：自由与互联网的未来
著者：[澳] 朱利安·阿桑奇
译者：Gavroche
出版发行：中信出版集团股份有限公司
（北京市朝阳区惠新东街甲4号富盛大厦2座 邮编100029）
电子书排版：萌芽图文

中信出版社官网： http://www.citicpub.com/
官方微博： http://weibo.com/citicpub
更多好书，尽在中信书院
中信书院：App下载地址 https://book.yunpub.cn/ （中信官方数字阅读平台）
微信号：中信书院

Table of Contents